APC 5M/APC 5M-12

取扱説明書

HYTEC INTER Co., Ltd.

第 1 版

管理番号:TEC-00-MA0203-01

ご注意

- 本書の中に含まれる情報は、弊社（ハイテクインター株式会社）の所有するものであり、弊社の同意なしに、全体または一部を複写または転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期して作成いたしましたが、万一、ご不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

改版履歴

第 1 版　2015 年 08 月 26 日　新規作成

ご使用上の注意事項

- 本製品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。
- 本製品を分解したり改造したりすることは絶対に行わないでください。
- 本製品を直射日光の当たる場所や、温度の高い場所で使用しないでください。本体内部の温度が上がり、故障や火災の原因になることがあります。
- 本製品を暖房器具などのそばに置かないでください。ケーブルの被覆が溶けて感電や故障、火災の原因になることがあります。
- 本製品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。
- 本製品を重ねて使用しないでください。故障や火災の原因になることがあります。
- 通気口をふさがないでください。本体内部に熱がこもり、火災の原因になることがあります。
- 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。
- 本製品の故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、弊社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。

目次

1. 製品概要 7

2. 梱包物一覧 7

3. ハードウェア 8

3.1. 各部名称 8
3.2. LED 9

4. アンテナ仕様（APC 5M-12） 10

5. インストレーション 11

5.1. ポール設置 11
5.2. 壁設置 14

6. 本マニュアルについて 16

7. システム構成例 18

7.1. ポイントーポイント 18
7.2. ポイントーマルチポイント 19

8. 初期設定 20

9. ネットワークの運用モード 22

9.1. ブリッジモードの初期設定例 23

10. マネジメントメニューについて 28

11. 設定変更の適用および設定変更の保存 31

12. 設定方法 32

12.1. Status 32
12.1.1. Information 32
12.1.2. Network 33

12.1.3. Wireless 34
12.1.4. Graphs 34
12.1.5. Route 35
12.1.6. ARP 35
12.2. Configuration 36
12.2.1. Network 36
12.2.1.1. Bridge モード 37
12.2.1.2. Router モード 40
12.2.2. Wireless 45
12.2.2.1. Access Point (auto WDS) 46
12.2.2.2. Access Point Repeater 51
12.2.2.3. Access Point iPoll 53
12.2.2.4. Station 57
12.2.2.5. Station(auto iPoll) 61
12.2.3. Virtual AP 64
12.2.4. Wireless ACL 66
12.2.5. Traffic Shaping 67
12.2.6. Port Forwarding 69
12.2.7. Static Routes 70
12.3. Services 71
12.3.1. WNMS 71
12.3.2. System alerts 72
12.3.3. SNMP 74
12.3.4. Clock/NTP 76
12.3.5. SSH 77
12.3.6. HTTP 77
12.3.7. Auto discovery 78
12.3.8. Ping watching 78
12.3.9. DHCP proxy 79
12.4. System 80
12.4.1. Administration 80
12.4.2. Log 82
12.4.3. LED 84
12.4.4. Firmware upgrade 85
12.5. Tools 86

12.5.1. Antenna alignment 86
12.5.2. Site survey 87
12.5.3. Delayed reboot 88
12.5.4. Ping 88
12.5.5. Trance route 89
12.5.6. Spectrum analyzer 90
12.5.7. Link test 91

13. ユニバーサルアクセス管理(UAM) 92

13.1 UAM 概要 92
13.2 UAM 設定 93
13.3 ホワイト/ブラックリスト 96

14. 付録 98

14.1 工場出荷モードへの設定方法 98
14.2 RADIUS 属性 99

15. 製品仕様 102

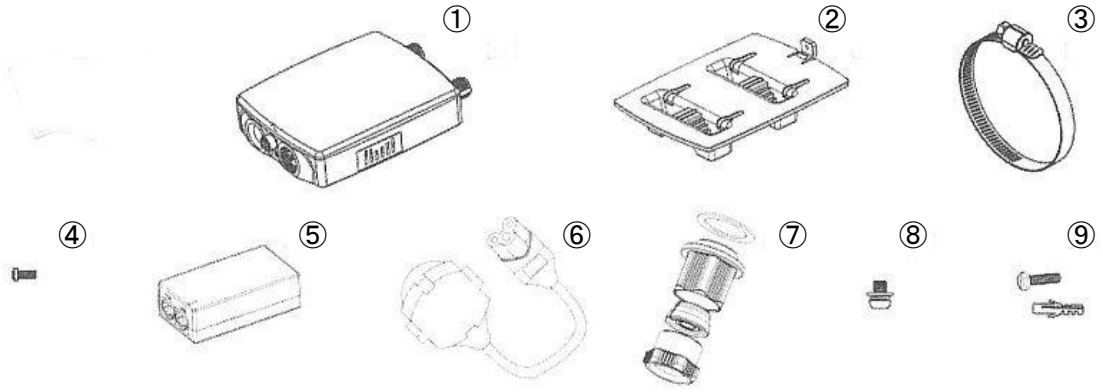
16. 製品保証 104

1. 製品概要

APC 5M-12 は、小型軽量の無線ブリッジです。本製品はポイントーポイントの他にポイントーマルチポイントの無線ブリッジとしても利用可能です。
IEEE802.11a/n に準拠しており屋内外で使用可能な為、様々なソリューションでお使いいただけます。

2. 梱包物一覧

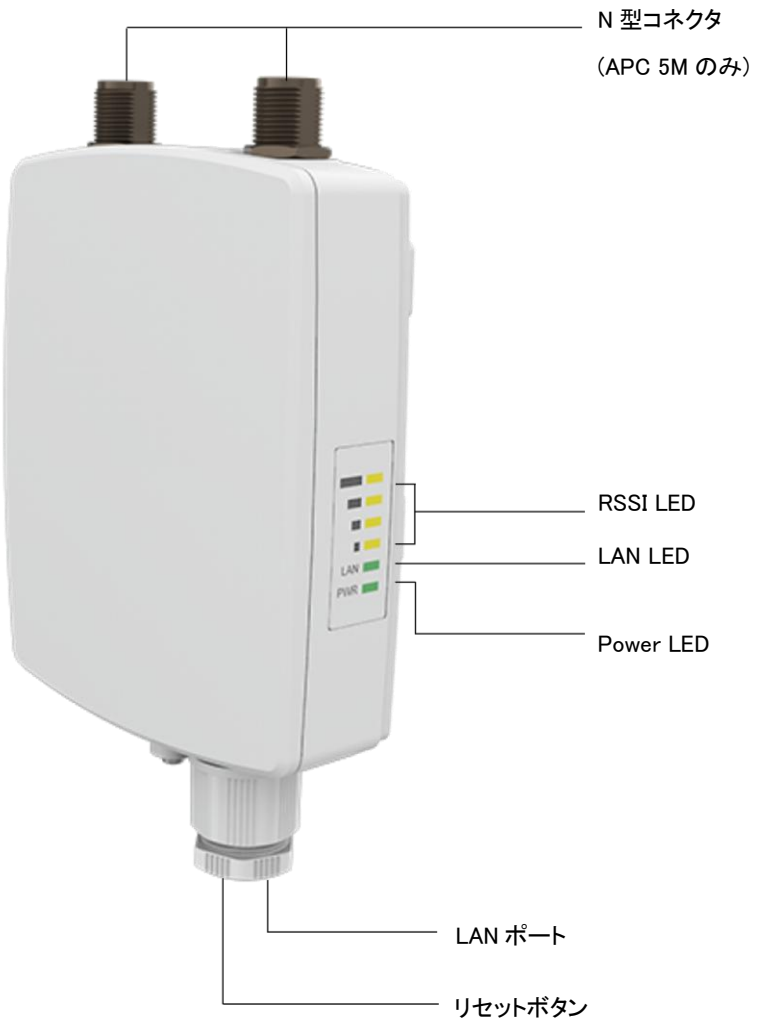
ご使用いただく前に本体と付属品を確認してください。万一、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。



#	名称	数量
①	APC 5M/APC 5M-12 本体	1
②	設置用ブラケット	1
③	ポール取り付け用クランプ	2
④	設置用ブラケット取り付けねじ	1
⑤	専用 PoE アダプタ	1
⑥	AC 電源ケーブル	1
⑦	LAN ケーブル取り付けパッキン	1
⑧	接地端子接続用ねじ	1
⑨	壁設置用ねじ＆アンカー	4

3. ハードウェア

3.1. 各部名称



◆ リセットボタン

背面のリセットボタンを押すことで、機器の再起動および初期化が可能です。

再起動・・・1秒長押し

初期化・・・5秒長押し

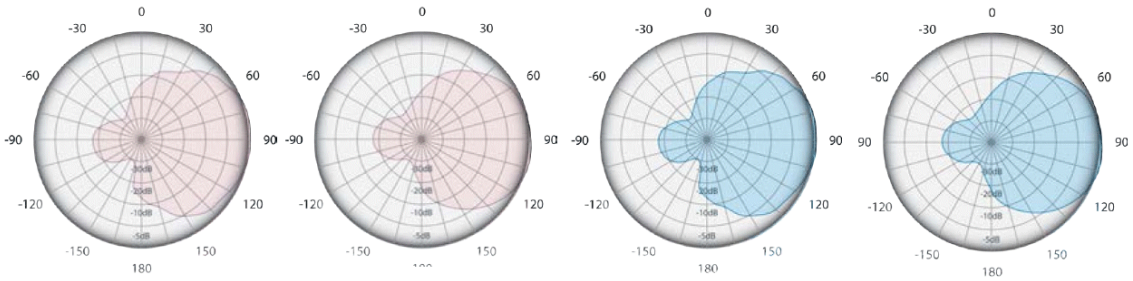
3.2. LED

本体側面には、電源、LAN、RSSI を確認できる LED があります。

#	LED 表示	状態	表示内容
①	PWR	**緑点灯**	電源が入っています。
		消灯	電源が入っていません。
②	LAN	**緑点灯**	イーサネットポートがリンクアップしています。
		消灯	イーサネットポートがリンクアップしていません。
		緑点滅	通信が行われています。
③	（RSSI）	**橙点灯**	クライアントからの電波の受信強度(RSSI)のレベルを表示します。

4. アンテナ仕様（APC 5M-12）

RF patterns (vertical)　　RF patterns (horizontal)



周波数帯域幅	4.9 – 5.0GHz
利得	12dBi
偏波極性	水平偏波/垂直偏波
偏波分離特性	22dB以上
VSWR	1.9以下
水平偏波水平方向半値角	60°
垂直偏波水平方向半値角	40°
垂直方向半値角	40°

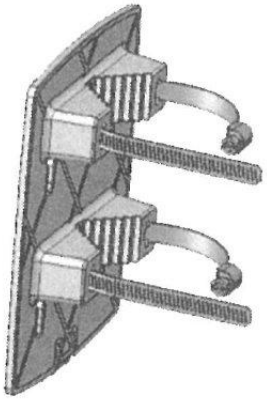
5. インストレーション

本製品には、ポールや壁取り付け用の部品が付属されています。
組み立てや設置の際は、以下の手順に従って作業してください。

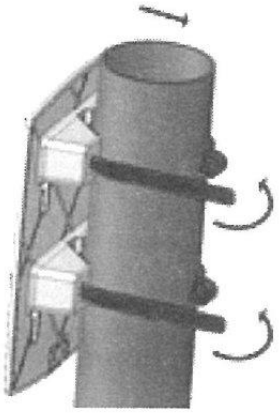
5.1. ポール設置

Step 1. 機器本体(B)の電源が入っていないことを確認して下さい。

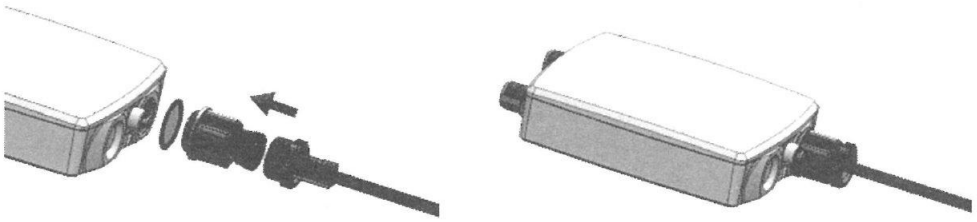
Step 2. 下図に示す通り、クランプ(D)を設置用ブラケット(C)に取り付けてください。



Step 3. クランプ(D)で設置用ブラケット(C)をポールへ確実に取り付けて下さい。

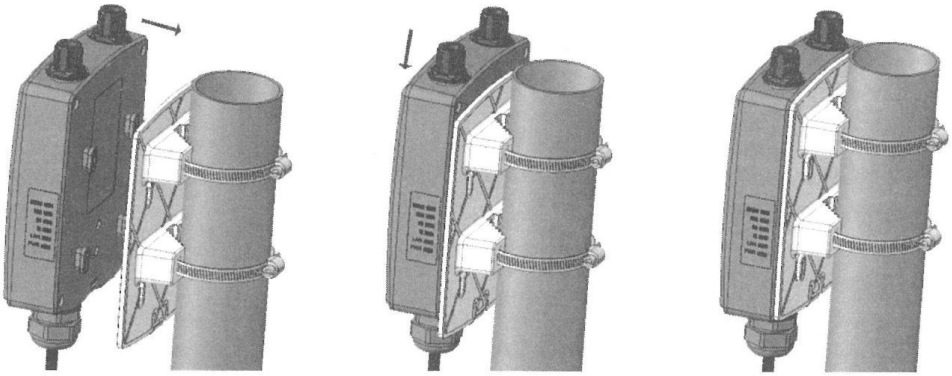


Step 4. 下図に示す通り、LAN ケーブルを APC 本体へ接続した後、ゴムガスケットをパッキン(H)に挿入しキャップで締めてください。



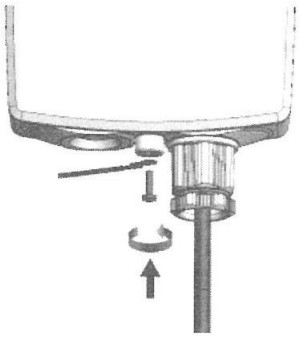
電磁ノイズの放射を減らす為に、STP ケーブルを使用することを推奨致します。

Step 5. 下設置用ブラケット(C)に APC 本体(B)を取り付け、下の方向へカチッと音が鳴るまではめ込んで下さい。



Step 6. 設置用ブラケット取り付けねじ(E)で APC 本体(B)を設置用ブラケット(C)に固定します。

Step 7. 雷保護としてAPC本体(B)を接地することができます。接地に使うリード線はAPC本体(B)の接地端子に必ず接地用ねじ(I)で接続して下さい。



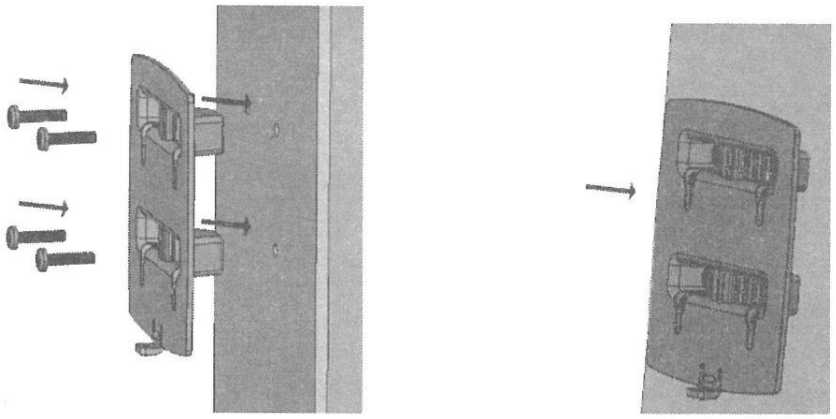
Step 8. 電源を投入します。付属のPoEインジェクタのPoEと記載のあるEthernetポートにEthernetケーブルを差し込み、そのケーブルを本体背面のEthernetポートに接続します。Power LEDが緑点灯になることを確認してください。(電源投入から数秒かかります)

動作中は、アンテナの正面に立たないでください。

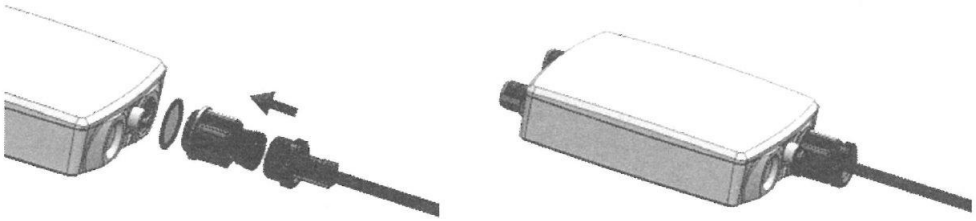
5.2. 壁設置

Step 1. 機器本体(B)の電源が入っていないことを確認して下さい。

Step 2. 下図に示す通り、設置用ブラケット(C)を壁接地用ねじ(J)で壁に取り付けてください。

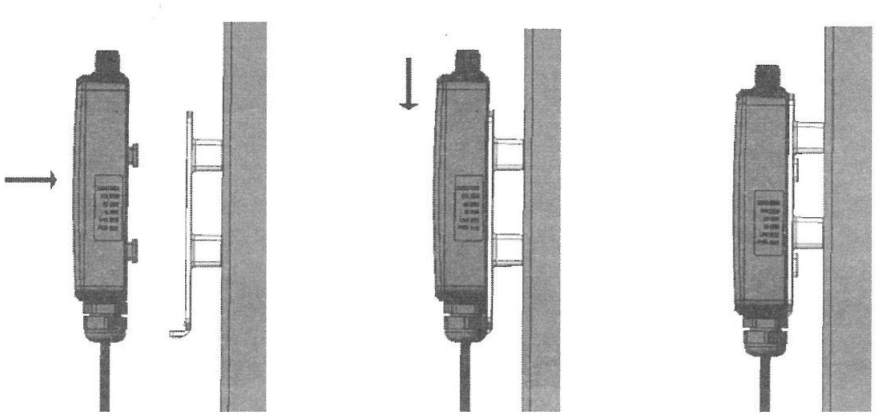


Step 3. 下図に示す通り、LAN ケーブルを APC 本体へ接続した後、ゴムガスケットをパッキン(H)に挿入しキャップで締めてください。



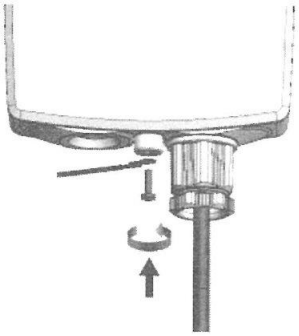
電磁ノイズの影響を低くするために、シールドされた STP ケーブルの使用をお勧めします。

Step 4. 下設置用ブラケット(C)に APC 本体(B)を取り付け、下の方向へカチッと音が鳴るまではめ込んで下さい。



Step 5. 設置用ブラケット取り付けねじ(E)で APC 本体(B)を設置用ブラケット(C)に固定します。

Step 6. 雷保護として APC 本体(B)を接地することができます。接地に使うリード線は APC 本体(B)の接地端子に必ず接地用ねじ(I)で接続して下さい。



Step 7. 電源を投入します。付属の PoE インジェクタの PoE と記載のある Ethernet ポートに Ethernet ケーブルを差し込み、そのケーブルを本体背面の Ethernet ポートに接続します。Power LED が緑点灯になることを確認してください。(電源投入から数秒かかります)

動作中は、アンテナの正面に立たないでください。

6. 本マニュアルについて

必要な技術と知識

本マニュアルを効率的に使う為には、LAN の概念と無線インターネット接続インフラの実用的な知識が必要です。

本マニュアルの表記規則

以下のシンボルが本マニュアルで使われています。

必須ではないが有益な追加情報です。

重要な情報であり注意してください。

略語リスト

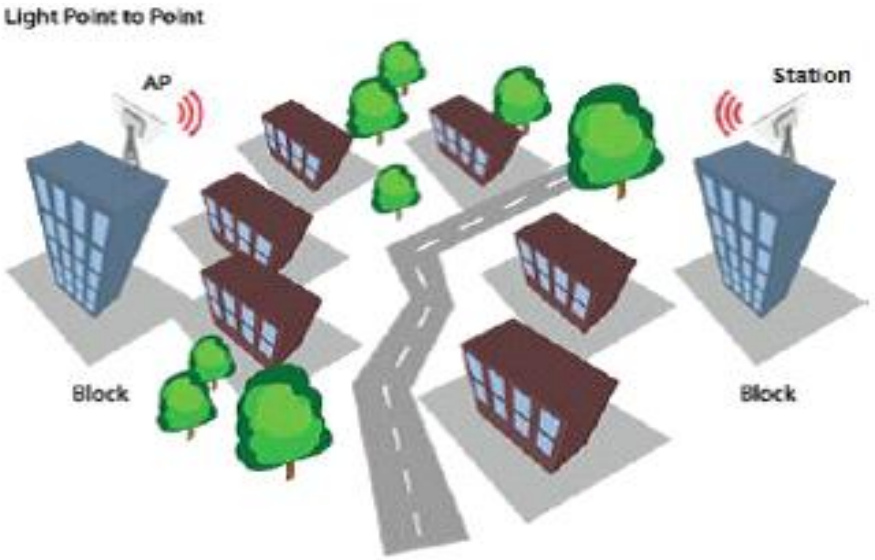
略語	詳細
ACL	Access Control List
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NAT	Network address translation – translation of IP addresses

	(and ports)
PC	Personal Computer
PDA	Personal Digital Assistant
PTP	Point To Point
PTMP	Point To Multi Point
PSK	Pre-Shared Key
QoS	Quality of Service
PEAP	Protected Extensible Authentication Protocol
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SISO	Simple Input, Simple Output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security (EAP-TTLS) protocol
TX	Transmission
UDP	User Datagram Protocol
UAM	Universal Access Method
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

7. システム構成例

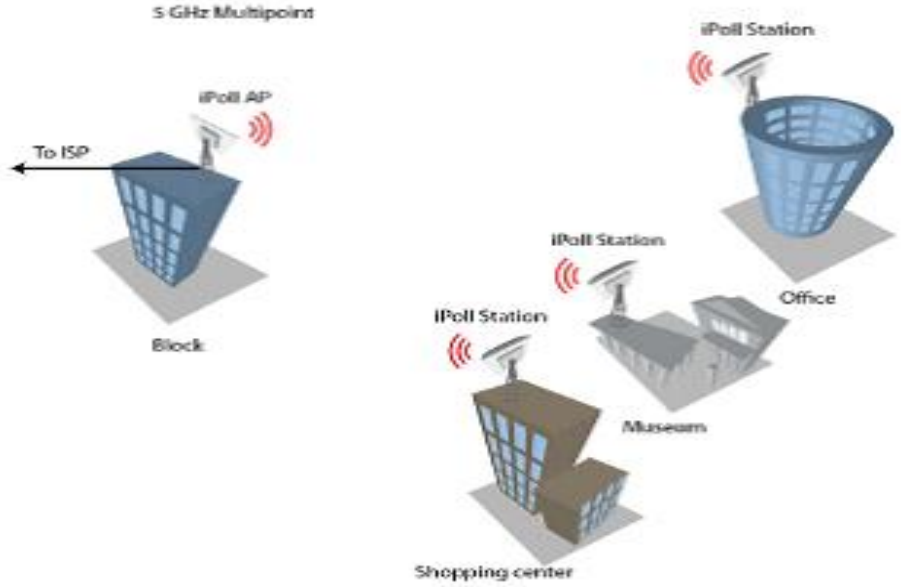
7.1. ポイントーポイント

本装置は、アクセスポイントモード(親機モード)とステーションモード(子機モード)を使用することでポイントーポイント接続が利用できます。



7.2. ポイントーマルチポイント

本装置は、iPoll プロトコルにより、1 つ以上の iPoll ステーション(子機)から iPoll アクセスポイント(親機)を連結するので、強力なポイントーマルチポイントネットワークが形成できます。



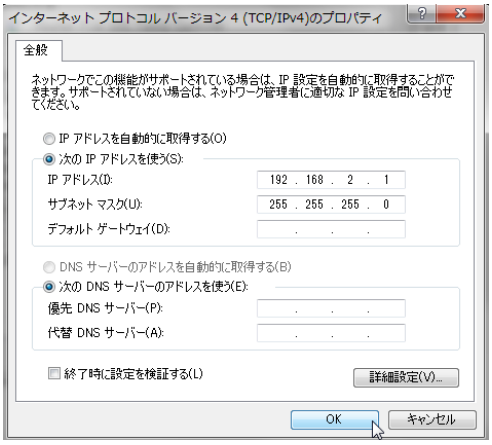
8. 初期設定

本装置の初期設定

IP アドレス　　:192.168.2.66

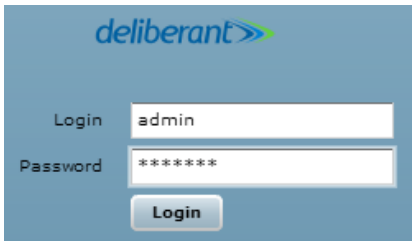
サブネットマスク:255.255.255.0

WEB ブラウザを使用して機器に接続するためには、パソコンの固定 IP アドレスを 192.168.2.1、サブネットマスクを 255.255.255.0 に設定します。



付属の PoE インジェクタの LAN と記載のある Ethernet ポートに Ethernet ケーブルを差し込み、そのケーブルをパソコンの Ethernet ポートに接続します。

WEB ブラウザに初期 IP アドレス 192.168.2.66 を入力すると、ログインページが表示されます。

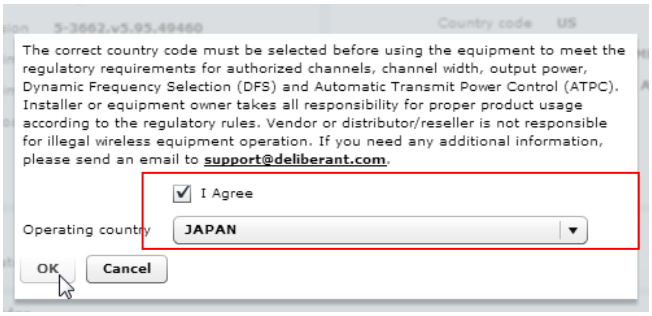


初期 ID、パスワード

Login　　:admin

Password　:admin01

初期ログイン時に、使用国の設定を行う必要があります。
必ず Operating Country に“JAPAN”が選択されていることを確認し、I Agree にチェックをいれて、OK ボタンを押してください。



※JAPAN 以外を使用すると、電波法違反となる恐れがあります。

9. ネットワークの運用モード

本装置は、以下の 2 つのモードを切り替えることにより、トランスペアレントブリッジやルータとして作動します。

・ブリッジモード(初期設定)

本装置は、無線ネットワークブリッジとして機能し、他の AP との無線リンクを確立することも可能です。このモードでは、全ての LAN ポートと無線インタフェースがブリッジの一部になります。

Figure 5 – Bridge Mode

ブリッジモードでは、接続された全てのパソコンが同じネットワークサブネット下になります。唯一ブリッジを渡れるデータは、反対側への有効なアドレスに送られるものだけになります。

・ルータモード

ルータモードでは、データをデバイスが WAN ポートを介して受け取り、別ネットワークの LAN ポートと共有します。WAN インタフェースへの接続タイプは Static IP、DHCP client または PPPoE client から作られます。

Figure 6 – Router Mode

デバイスがルータモードで作動する際、有線インタフェースで入ってくるトラフィックや、無線インタフェースで出ていくトラフィックは、NAT を利用することで隠すことができます。インターネット上の他のクライアントたちには、この出ていく全てのトラフィックが AP から出ているようにみえます。

9.1. ブリッジモードの初期設定例

まず本製品を二台用意し、一方を AP(Access Point)として設定します。

ステップ 1　　LAN ケーブルでパソコンと AP を接続して下さい。

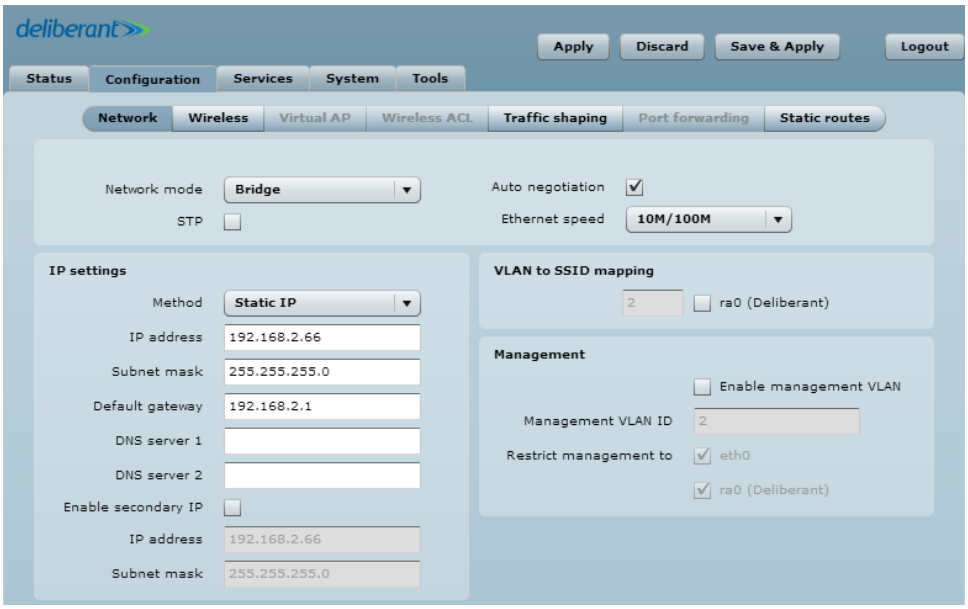
ステップ 2　　パソコンが AP のサブネットにセットされているかを確認してください。
（例）192.168.2.150

ステップ 3　　WEB ブラウザを開いて IP アドレスを指定してください。

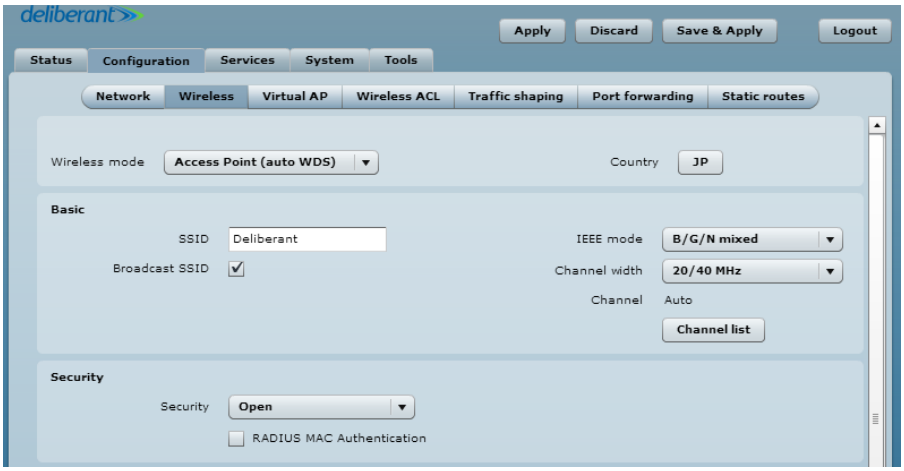
ステップ 4　　初期設定（192.168.2.66/24）

ステップ 5　　初期パスワードを入力し、Login ボタンを押してください。

ステップ 6　　Configuration/Network タブをクリックし、Network mode は Bridge を選択し、IP settings の Method で Static IP を選択した後 Save & Apply をクリックしてください。



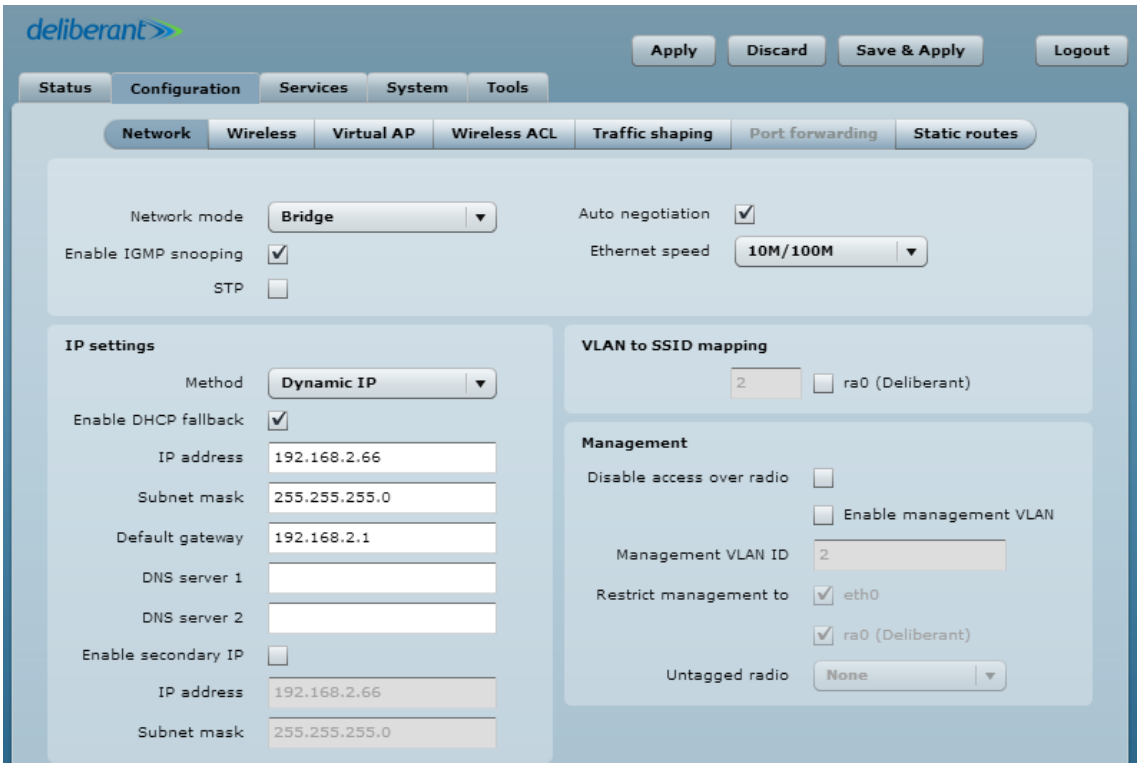
ステップ 7　　Configuration/Wireless タブをクリックし、Wireless mode は Access Point(auto WDS)を選択、Broadcast SSID にチェックを入れて、Security と IEEE mode をそれぞれ任意に選択して Save & Apply をクリックしてください。



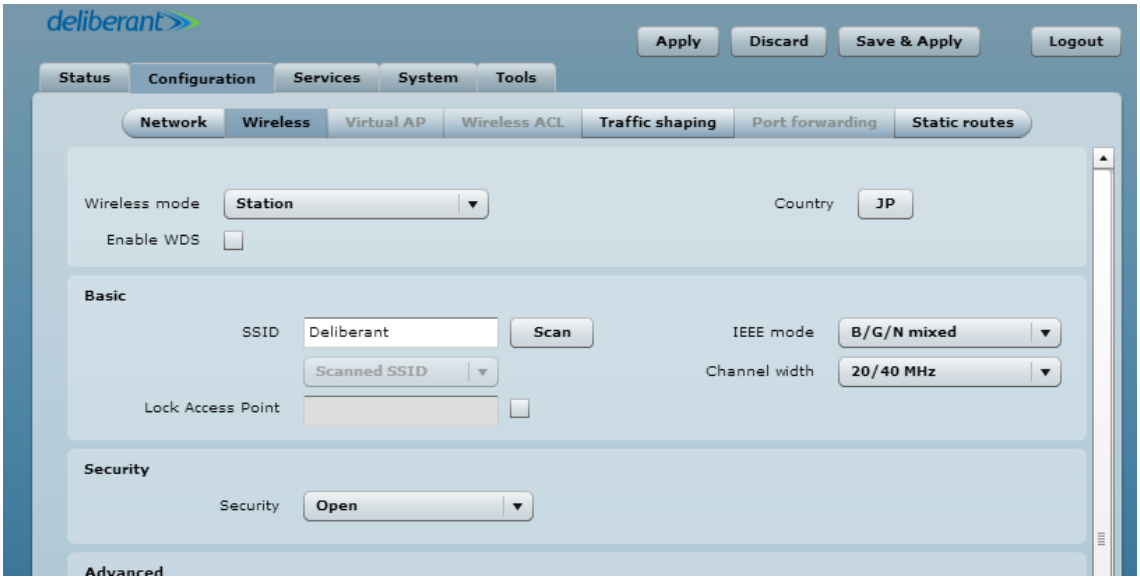
次に本製品のもう一方を無線クライアント(子機)として設定します。

ステップ 1～5 は、AP の初期設定例と同じです。

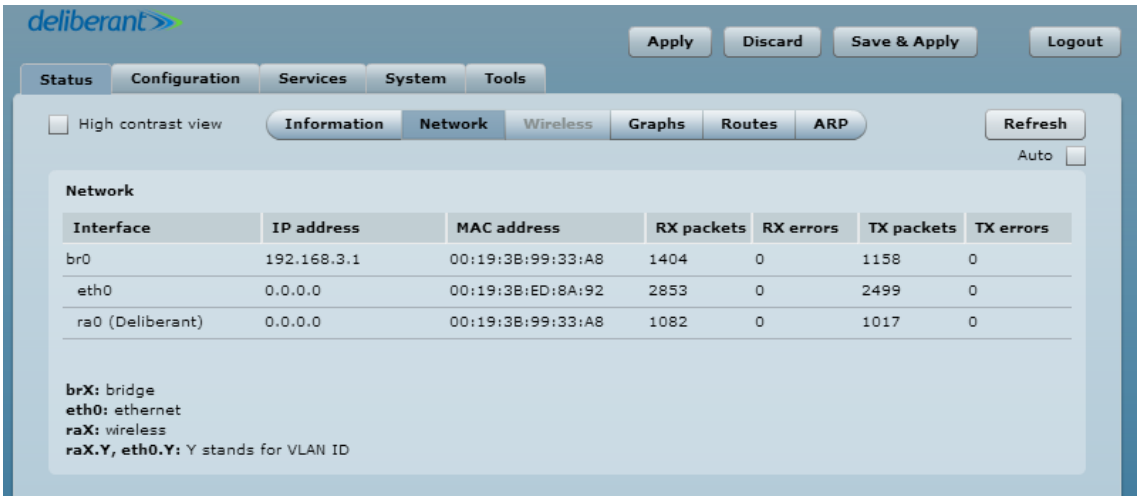
ステップ 6　　Configuration/Network タブをクリックし、Network mode は Bridge を選択し、IP settings の Method で Static IP を選択した後 Save & Apply をクリックしてください。AP とは違う IP アドレスに変更しておくと管理上有益です。



ステップ 7　　Configuration/Wireless タブに移動、wireless mode は Station を選択し、SSID 入力欄の近くの Scan ボタンをクリックしステーションと接続する AP の SSID を選択します。AP に対する Security パラメータ選択し、IEEE モード(これらのセッティングは必ず AP 無線セッティングに従う)をチェックして、Save & Apply をクリックしてください。



ステップ 8　　接続を確認するため、Status/Network ページに移動してください。Network ページは、AP に関するメイン・ネットワーク・インフォメーションを表示します。



ステップ 9　　Status/Information ページでは、アクセスポイントとのリンク情報を表します。

10. マネジメントメニューについて

システムへのログイン後、マネジメントメニューが表示されます。
このメニューから、システムを設定する全ての必要なページにアクセスすることができます。
有効なタブは、異なる色で表示されます。

マネジメントメニューの構成は以下のとおりです。

◆Status

Information	装置の概要を表示します。
Network	メインネットワークおよび wireless の統計値を表示します。
Wireless	特定のインタフェースに接続された端末の情報を表示します。
Graphs	使用中の Wireless および Ethernet のトラフィックをグラフで表示します。
Routes	装置のルーティングテーブルを表示します。
ARP	ARP テーブルを表示します。

◆Configuration

Network	network mode、 Ethernet speed、IP settings、 management and data VLANs、DHCP、PPPoE を設定します。
Wireless	wireless mode、country、SSID、IEEE mode、channel configuration、security、advanced radio を設定します。
Virtual AP	仮想 AP の設定(AP wireless モードのみ)を行います。
Wireless ACL	MAC アドレスによるアクセスコントロールを行います。 (AP および iPoll wireless モードのみ)
Traffic shaping	ダウンロードおよびアップロードトラフィックの制御を行います
Port forwarding	ポートフォワーディングの規則を設定します。 (AP および iPoll AP のルータ・ネットワーク モードのみ)
Static routes	スタティックルーティングの規則 を設定します。 (AP および iPoll AP のルータ・ネットワーク モードのみ)

◆Services

WNMS	WNMS を設定することにより server/collector URL でリモート側装置の設定および監視が可能になります。
System Alerts	System Alerts を設定することにより装置の警報を SNMP トラップあるいは SMTP の通知として送ることができます。
SNMP	SNMP を設定することによりリモート側装置を監視することができます
Clock/NTP	装置の時刻を行います。 設定はマニュアル設定または NTP サービス利用するかを選択します。
SSH	SSH 接続の制御を行います。
HTTP	HTTP 接続の制御を行います。
Auto discovery	制御装置の自動検出機能を設定します。
Ping watchdog	指定したホストとのネットワーク接続が失われた場合、自身を再起動します。
DHCP proxy	DHCP リレーエージェントとして動作するよう設定します。

◆System

Administration	パスワードの変更、リブート、初期化、設定値のバックアップおよびインストールを行います。
Log	ログの確認、ログの転送設定を行います。
LED	LED の操作制御を行います。
Firmware upgrade	ファームウェアのアップグレードを行います。

◆Tools

Antenna alignment	ワイヤレスネットワークの受信信号の品質を測定しアンテナ設置の調整を行います。
Site Survey	同じ地域に存在するワイヤレスネットワークの情報を表示します
Delayed reboot	装置の再起動関わる遅延時間設定を行います。
Ping	ping コマンドを実行します。
Trace route	Trace route コマンドを実行しその結果をグラフィカルに表示します。
Spectrum analyzer	利用可能なチャネルの信号の強さを確認します。
Link test	リンク状態の品質確認を行います。

11. 設定変更の適用および設定変更の保存

Apply **– Apply ボタンがクリックされると新しい設定が即座に適用されます。数秒後に装置は新しい設定で稼働します。しかし、新しい設定はメモリに記憶されてはいないため、装置が再起動した場合、装置は古い設定で起動します。**

Discard **–Discard ボタンがクリックされると変更されたパラメータは破棄されます。しかし、Apply ボタンあるいは Save & Apply ボタンがクリックされていた場合、パラメータは破棄されません。**

Save & Apply **– Save & Apply ボタンがクリックされると新しい設定が即座に適用されメモリに記憶されます。**

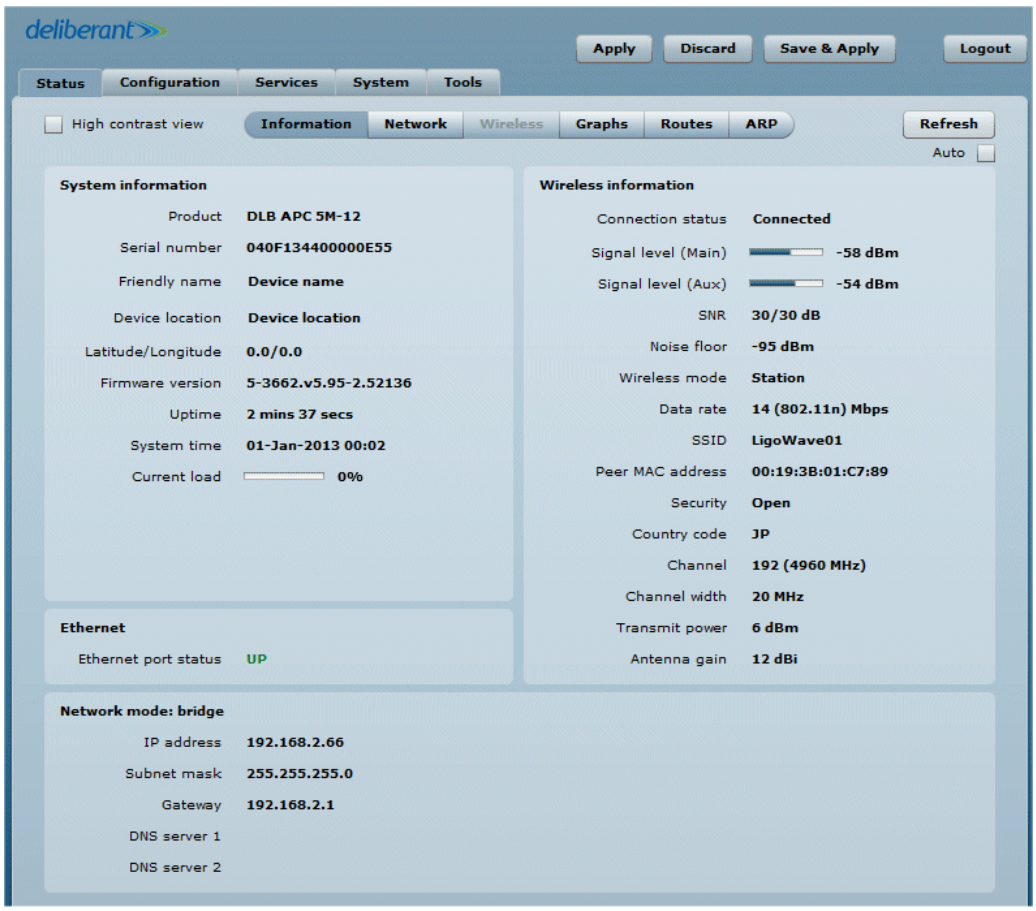
パラメータを変更した Web GUI タブごとに Apply ボタンまたは Save & Apply ボタンをクリックする必要はありません。
各 Web GUI ダブでパラメータ変更が完了した後で Apply ボタンまたは
Save & Apply ボタンをクリックすることにより設定変更は提供されます。

12. 設定方法

12.1. Status

12.1.1. Information

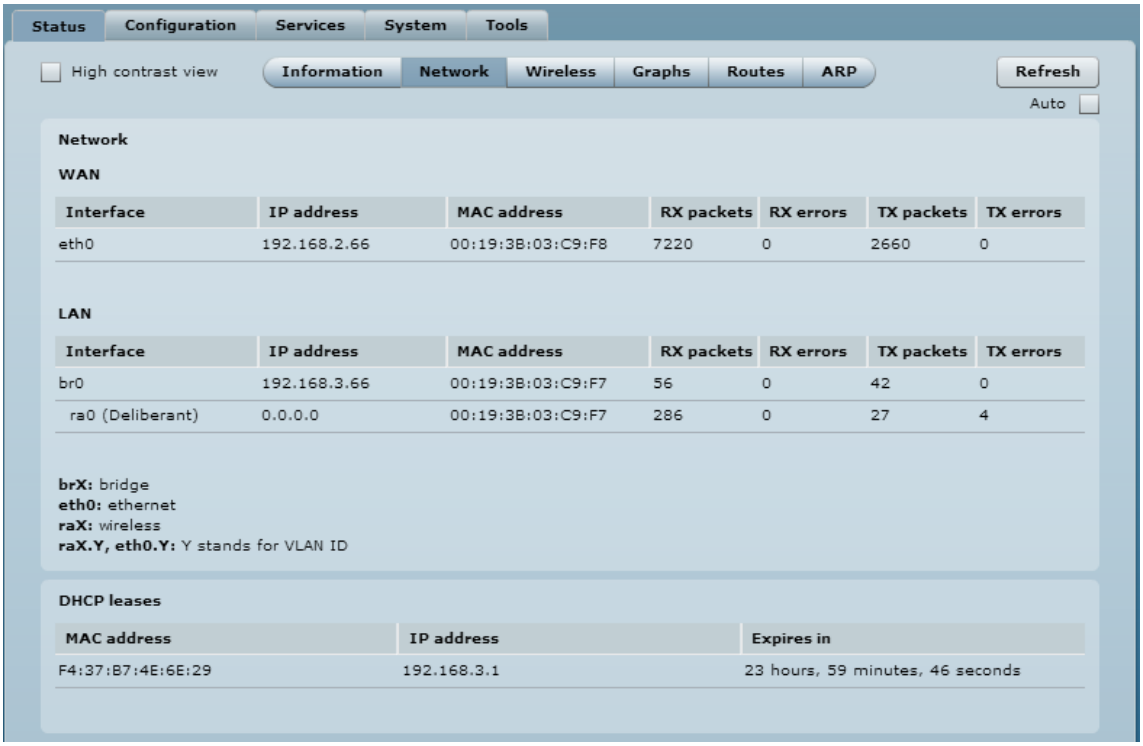
Information ページは本装置の状態の概要を表示します。本装置の運用モードやネットワーク設定の重要な情報が表示されます。



項目	内容
System information	本装置の全般的な情報が表示されます。
Wireless information	ワイヤレスネットワークについての全般的な情報が表示されます。 情報は、Wireless モードにより異なります。
Ethernet	イーサネットポートのリンク状態を表示します。
SSID details	SSID とセキュリティタイプを表示します。
Network mode	現在のネットワーク設定概要を表示します。

12.1.2. Network

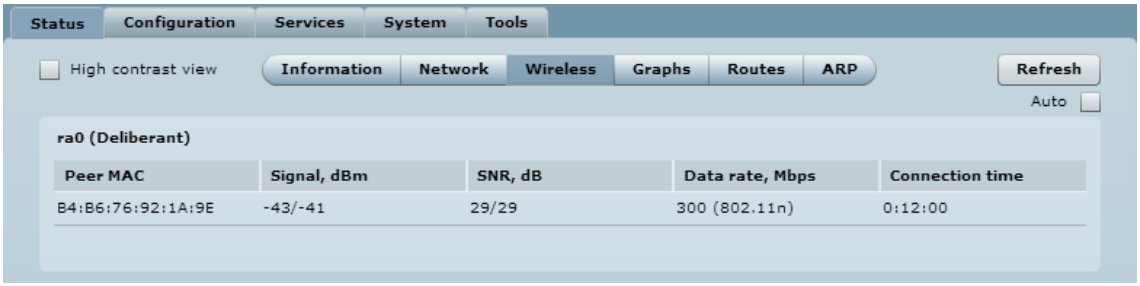
Network では各インタフェースの統計情報および DHCP リースについて表示します。(表示内容はネットワークモードによります。)



項目	内容
Interface	インタフェース名を表示します。
IP address	各インタフェースの IP アドレスを表示します。
MAC address	各インタフェースの MAC アドレスを表示します。
RX packets	受信パケット数を表示します。
RX errors	受信データのエラー数を表示します。
TX packets	送信パケット数を表示します。
TX errors	送信データのエラー数を表示します。
DHCP leased	DHCP 機能でリースされている IP アドレスの情報を表示します。

12.1.3. Wireless

Station wireless mode で運用されている場合、Status Wireless は機能しません。

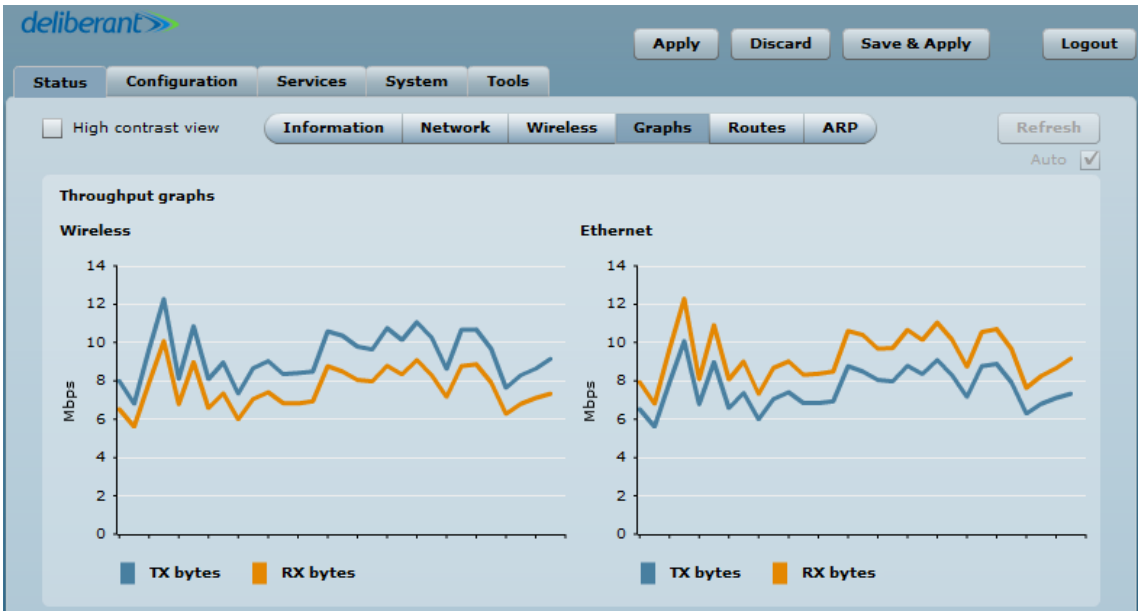


項目	内容
Peer MAC	AP に接続された端末の MAC アドレスが表示されます。
Signal	AP が通信する station 間のシグナルの強さを dBm で表示します。
SNR	ノイズのレベルを dBm で表示します。
Data rate	アクセスポイントが通信している station 間のデータレートを表示します。
Connection time	セッションの継続時間を表示します。

12.1.4. Graphs

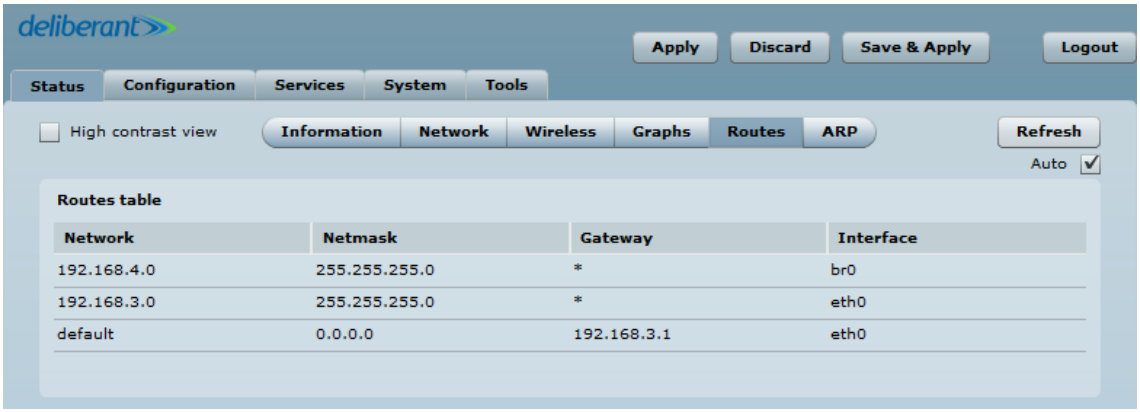
Ethernet と Wireless インタフェースのリアルタイムトラフィックデータを表示します。

グラフは 5 秒間隔で更新されます。



12.1.5. Route

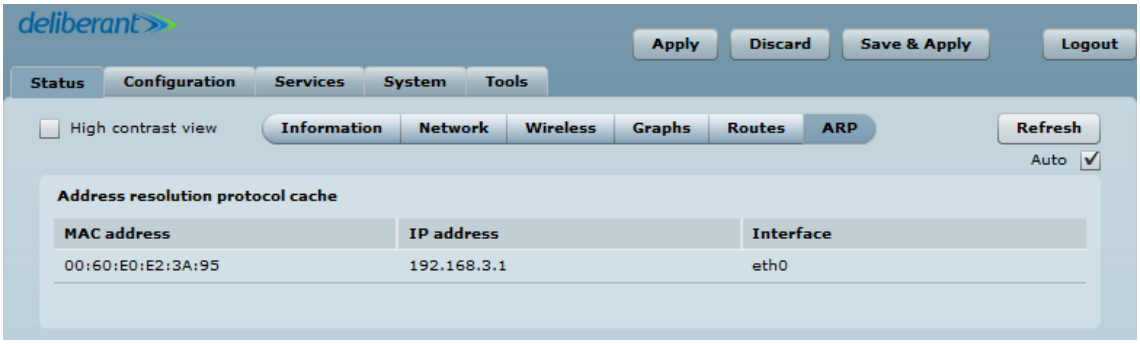
各インタフェースのルーティングテーブルを表示します。



12.1.6. ARP

現在保存されている ARP table を表示します。

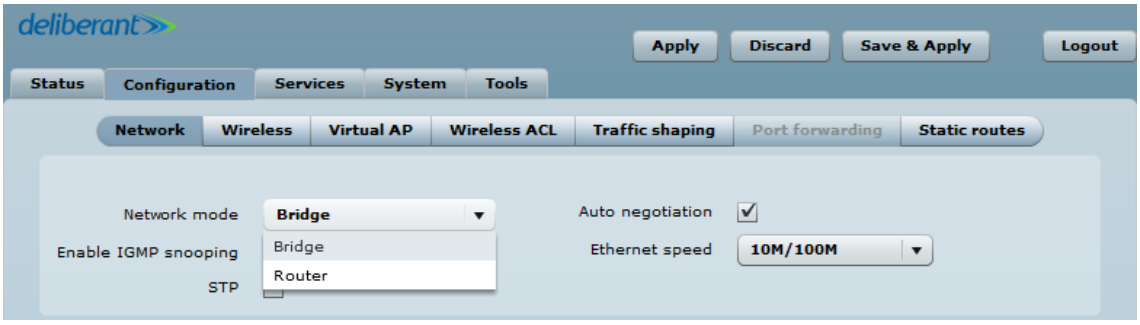
Refresh button をクリックすると ARP table が再読み込みされます。



12.2. Configuration

12.2.1. Network

Configuration の Network ページで network の設定を行います。最初に運用モードを定義します。運用モードは、Bridge 又は Router を選択します。

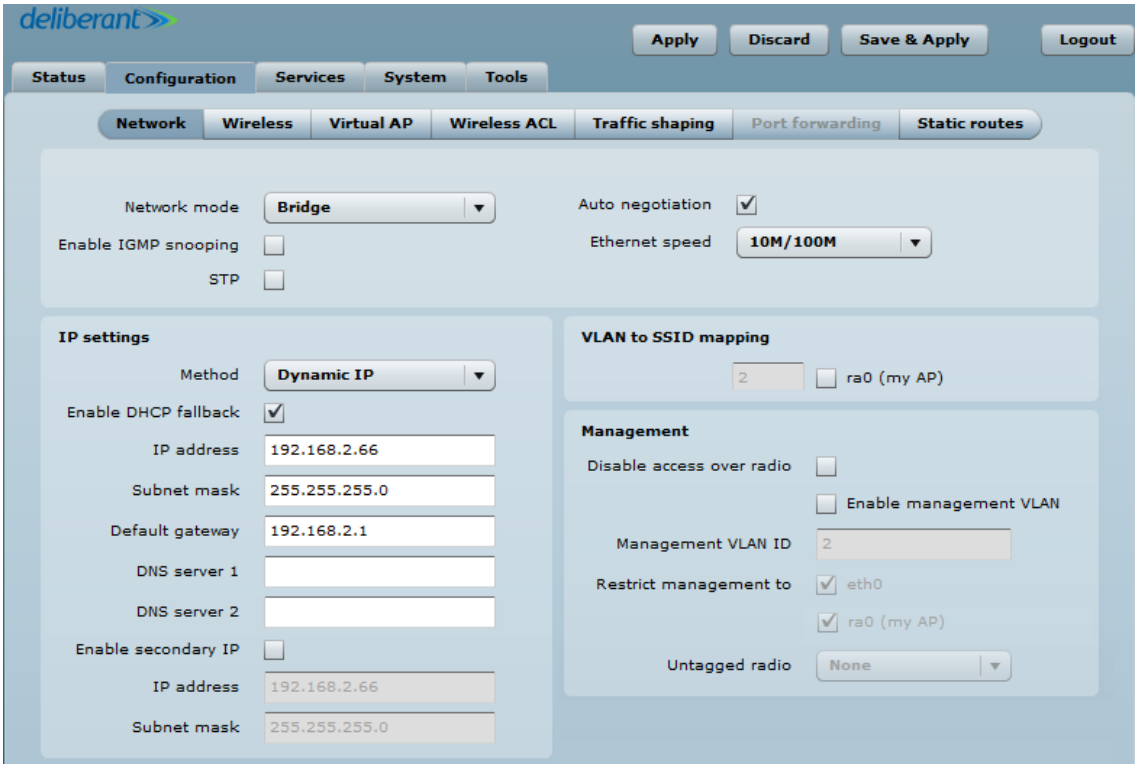


項目		内容
Network mode		運用モードの選択で Bridge 又は Router を選択します。
	Bridge	ブリッジモードでは、トランスペアレントブリッジとして動作し、ワイヤレスネットワークと LAN ポートを相互接続します。
	Router	ルータモードでは、ワイヤレスネットワークと全ての LAN ポートの間でルータとして動作します。

12.2.1.1. Bridge モード

Port forwarding と Static routes は、Bridge モードではご使用になれません。

Bridge モードでは、LAN セッティングのみ表示されます。



項目	内容
IGMP snooping （AP、iPoll Bridge モードのみ）	IGMP スヌーピング機能を有効にするか選択します。 有効にした場合、AP はクライアントとマルチキャストホスト間で転送されたパケットをスヌーピングしてグループ登録情報を取り出し、MAC アドレステーブルに登録します。 そのテーブルにしたがって、マルチキャストトラフィックを転送します。
STP	スパニングツリープロトコル（STP）を有効にするか選択します。
Auto negotiation	Ethernet リンクの自動検出の選択を行います。
Ethernet speed	自動検出を無効にした場合、Ethernet リンクの固定設定を行います。

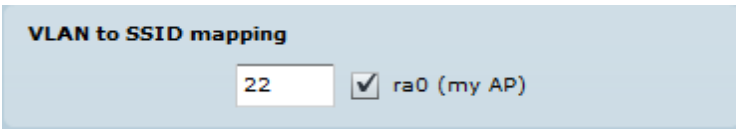
IP Setting

AP に設定する予定の IP アドレスが、有線 LAN と同じネットワークに属しており、他で利用されていないことを確認してください。間違えて設定した場合、AP に接続できなくなります。

DHCP client 機能を有効に設定している場合、新しい設定を保存したあとDHCP サーバから割り当てられる IP アドレスが分からない為、ブラウザの接続が切断れます。

項目		内容
Method		IP アドレス割り当ての方法を設定します。
	Static IP	IP アドレスを任意に設定します
	Dynamic IP:	IP アドレスは DHCP サーバから割り当てられます。 DHCP サーバから IP アドレスが割り当てられない場合、本装置は fallback IP アドレスを利用します。 Fallback IP アドレスは、192.168.2.66 です。 Fallback IP アドレスは変更することができます。
IP Address		本装置の IP アドレスを設定します。
Subnet mask		subnet mask を設定します。
Default gateway		default gateway IP アドレスを設定します。
DNS server1/2		DNS server の IP アドレスを設定します。
Enable secondary IP		予備の IP アドレスおよびサブネットマスクを設定します。

VLAN to SSID Mapping

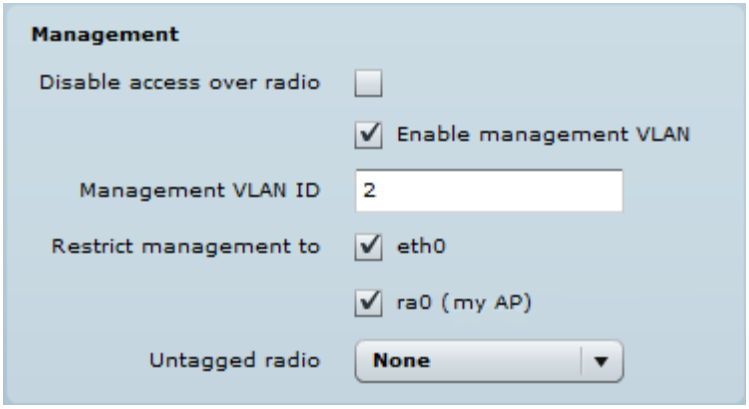


項目	内容
VLAN to SSID Mapping	VLA ID は特定の radio interface の traffic tagging のために設定します [2-4095]。特定の SSID を使用する Station は、この VLAN にグルーピングされます。

Network Management

この機能は Bridge network mode の時のみ機能します。

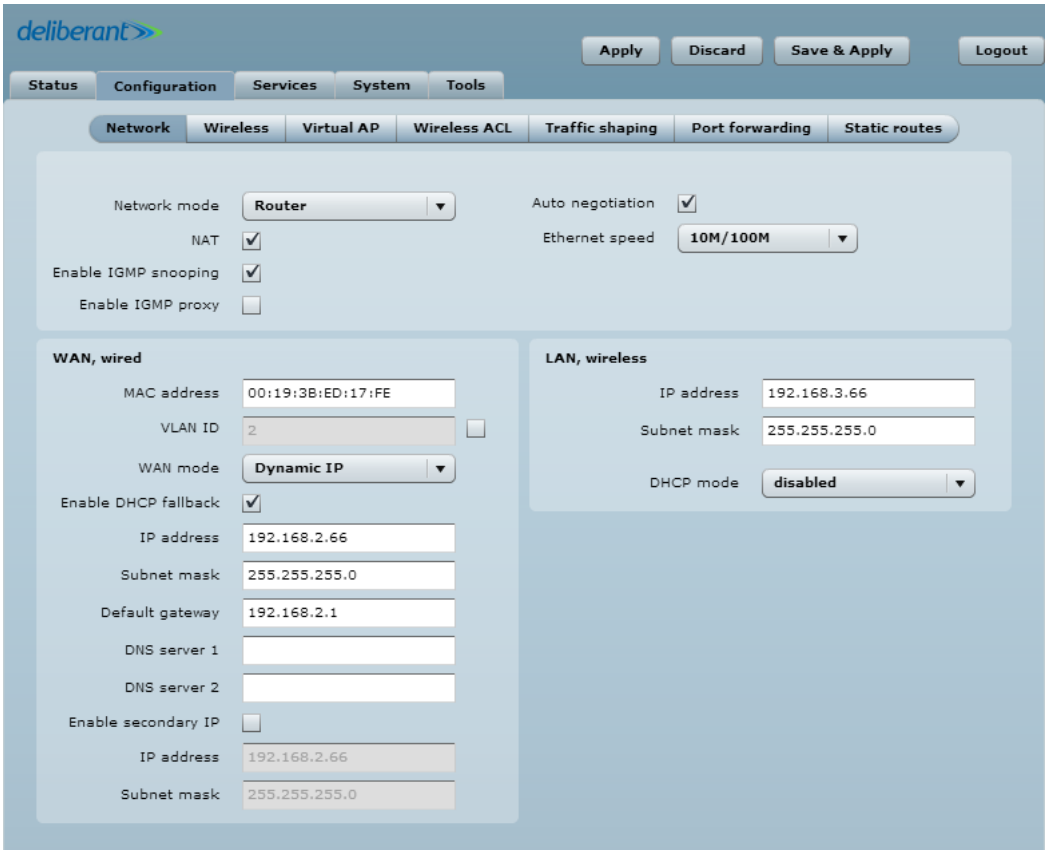
新しい管理用 VLAN を設定すると、本装置への HTTP 接続が切れます。
このため、新しい管理 VLAN で管理ステーションを接続するか、マルチ VLAN ルータを介して新しい管理 VLAN に接続します。



項目	内容
Disable access over radio	ワイヤレス経由での管理アクセスを無効にします。 AP への管理アクセスは、VLAN タグを使用して 制限することができます。 管理 VLAN を定義することによって、 デバイスは適切な管理 VLAN ID を持つフレームのみを受け入れます。
Enable management VLAN	管理用トラフィックのために VLAN tagging を有効にします。
Management VLAN ID	VLAN ID を設定します。本装置のインタフェースに VLAN ID が設定されるとその VLAN ID と適合した管理用フレームのみを装置は受け付けます。
Restrict management to interface	管理用 VLAN を適用するインタフェースを選択します。
Untagged radio	Untagged ポート選択します。

12.2.1.2. Router モード

このセクションでは DHCP サーバ機能を含むルータのパラメータ設定を行います。本装置をルータとして運用する場合、WAN network 設定、LAN network 設定、LAN DHCP 設定を行う必要があります。

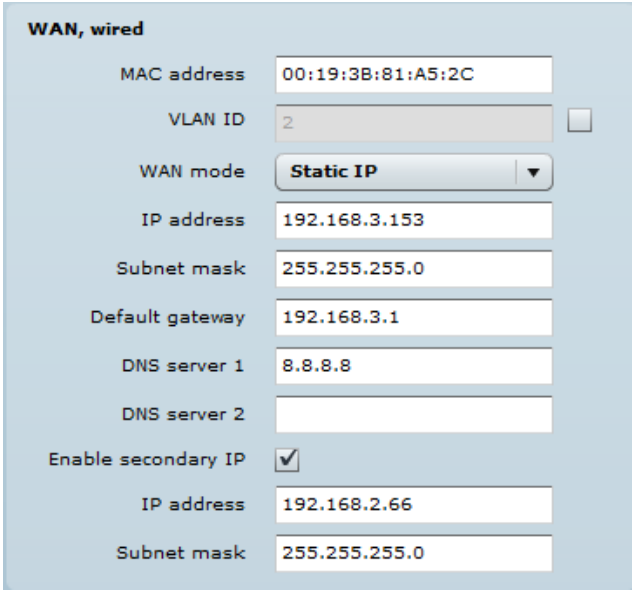


項目	内容
Enable NAT	NAT 機能を有効にします。
Enable IGMP snooping	IGMP スヌーピング機能を有効にするか選択します。 有効にした場合、AP はクライアントとマルチキャストホスト間で転送されたパケットをスヌーピングしてグループ登録情報を取り出し、MAC アドレステーブルに登録します。 そのテーブルにしたがって、マルチキャストトラフィックを転送します。
Enable IGMP proxy	IGMP プロキシ機能を有効にします。 IGMP インタフェースを介して検出された IGMP ホストの プロキシとして動作します。
Auto negotiation	Ethernet リンクの自動検出の選択を行います。
Ethernet speed	自動検出を無効にした場合、Ethernet リンクの固定設定を行います。

WAN Setting

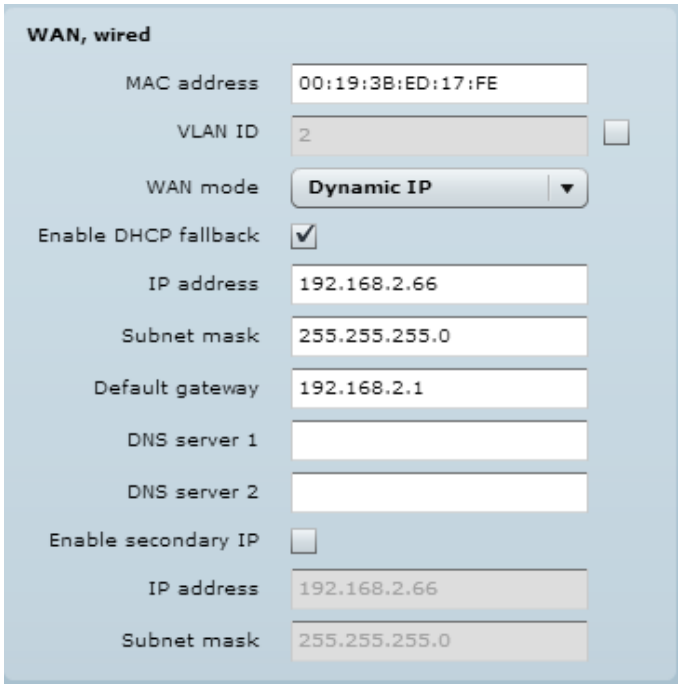
WAN interface に関係する設定を含む WAN network の設定を行います。WAN interface のアクセスタイプを Static IP, Dynamic IP, PPPoE client から選択します。

WAN mode – 本装置の WAN interface に **Static IP** を選択した場合



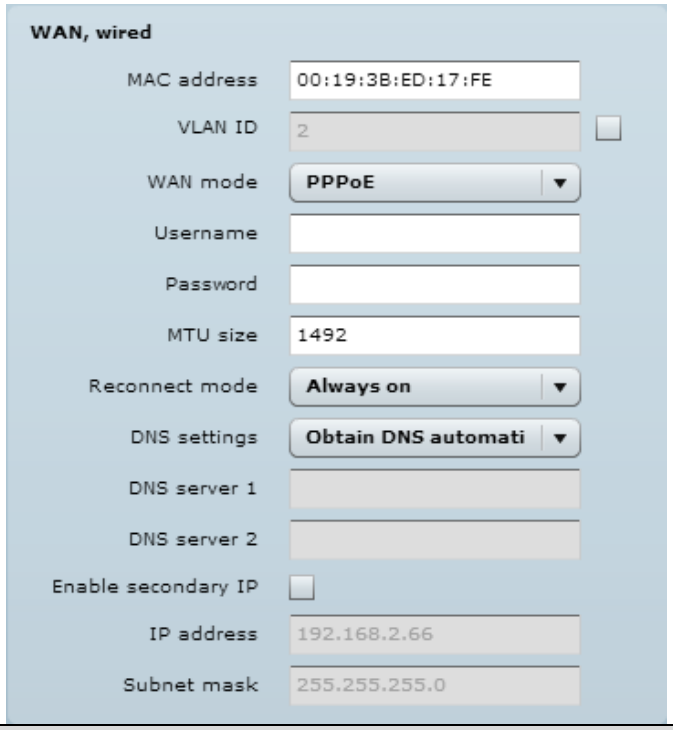
項目	内容
MAC address	この値は変更しないでください。
VLAN ID	無線インタフェースの VLAN ID を指定します。[2-4095]
IP address	本装置の IP アドレスを設定します。
Subnet mask	subnet mask を設定します。
Default gateway	default gateway IP アドレスを設定します。
DNS server	DNS server の IP アドレスを設定します。
Enable secondary IP	予備の IP アドレスおよびサブネットマスクを設定します。

WAN mode – **Dynamic IP** を選択し WAN 側の DHCP client を有効にします。このオプションに関するパラメータは有りません。



項目	内容
MAC addles	この値は変更しないでください。
VLAN ID	無線インタフェースの VLAN ID を指定します。[2-4095]
DHCP fallback setting	IP アドレス, サブネットマスク, デフォルトゲートウェイ およびオプションとして DNS サーバを DHCP フォールバックのために設定します。 本装置が DHCP サーバから IP アドレスを取得できない場合、設定されたフォールバック IP アドレスが使われます。
Enable secondary IP	予備の IP アドレスおよびサブネットマスクを設定します。

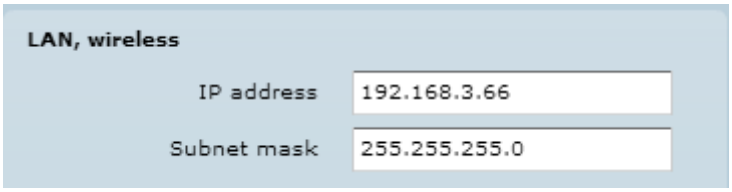
WAN mode -PPPoE ※本設定はサポート対象外です



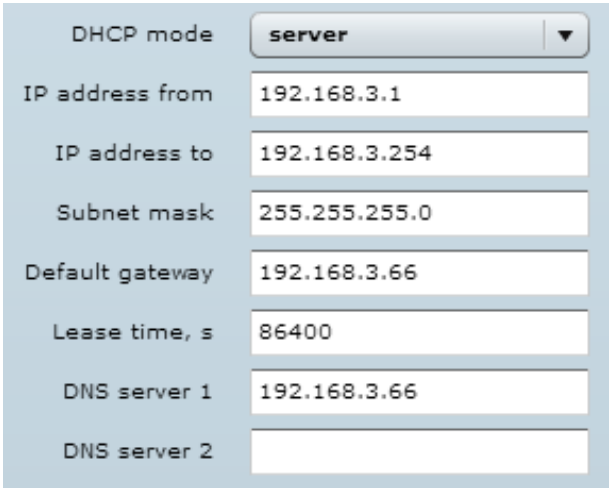
項目	内容
MAC addles	この値は変更しないでください。
VLAN ID	無線インタフェースの VLAN ID を指定します。[2-4095]
User name	PPPoE のユーザネームを設定します。
Password	PPPoE のパスワードを設定します。
MTU	MTU(Maximum Transmission Unit)を入力します。 MTU の初期値は 1500bytes です。
DNS setting	DNS サーバの IP アドレスを自動的に取得するかマニュアルで設定するかを選択します。
Enable secondary IP	装置の管理用の代替の IP アドレスおよびサブネットマスクを設定します。

LAN Network Setting

LAN interface を含む LAN network についての設定



項目	内容
IP address	装置の LAN interface に IP address を設定します。
Subnet mask	装置の LAN interface に Subnet mask を設定します。
DHCP mode	
disable	DHCP は無効になります。
relay	DHCP リレーとして動作します。
server	DHCP サーバとして動作します。

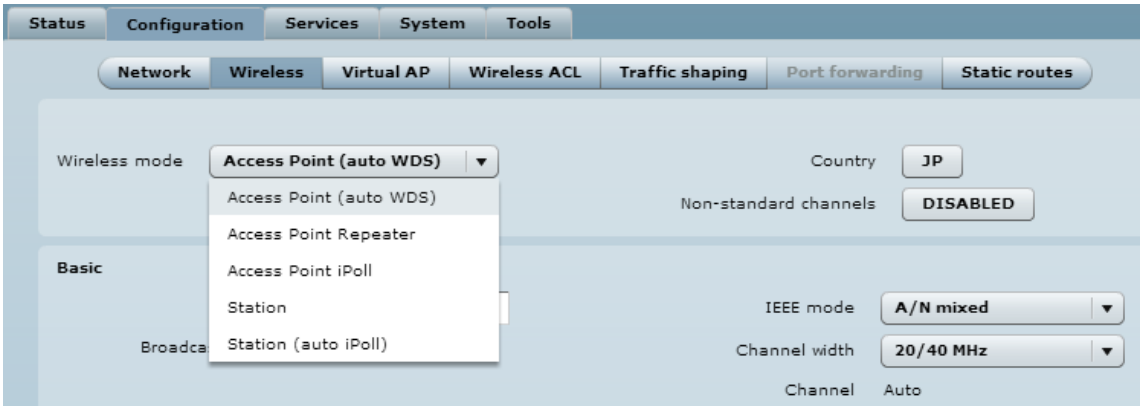


項目	内容
IP address from	DHCP アドレスプールの開始 IP アドレスを設定します。
IP address to	DHCP アドレスプールの最終 IP アドレスを設定します。
Subnet mask	サブネットマスクを設定します。
Default gateway	デフォルトゲートウェイを設定します。
Lease time	DHCP サーバから割り当てる IP アドレスの有効期限を秒単位で設定します。
DNS server	DNS サーバの IP アドレスを設定します。

12.2.2. Wireless

Wireless のセクションは 3 つのパートに分かれています。Basic, Security および Advanced です。Basic セクションは、wireless link に関わる全ての設定パラメータを含みます。Security セクションでは、認証および暗号化の設定を行います。Advanced セクションには、link 収容能力を最適化するパラメータがあります。

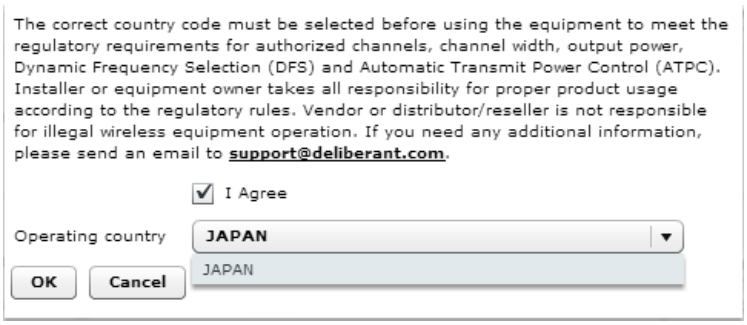
Wireless mode – 本装置の運用モードの違いによりいくつかの設定パラメータが異なります。
（たとえば、security または advanced wireless 設定）



項目	内容
Access Point (auto WDM)	本装置の無線機能をアクセスポイントとして使います。 本装置が **Access Point(auto WDS)** モードで設定されると、端末は AP からのブロードキャストを受信し、設定が適切であれば AP と通信が可能となります。
Access Point Repeater	AP の無線信号の範囲を拡張するための無線中継器として動作が可能になります。
Access Point iPoll	iPoll は独自機能です。最適化を行い、スループット等を向上させます。 クライアントは **Station(auto iPoll)** 設定の APC 5M-12 のみ接続可能です。
Station	無線機能をクライアントモードに設定します。 このモードでは、SSID はブロードキャストされず、クライアントは本装置に接続することはできません。 AP で稼働しているアクセスポイントに接続することができます。
Station(auto iPoll)	**Access Point iPoll** 設定の APC 5M-12 と接続するクライアントとして使用します。

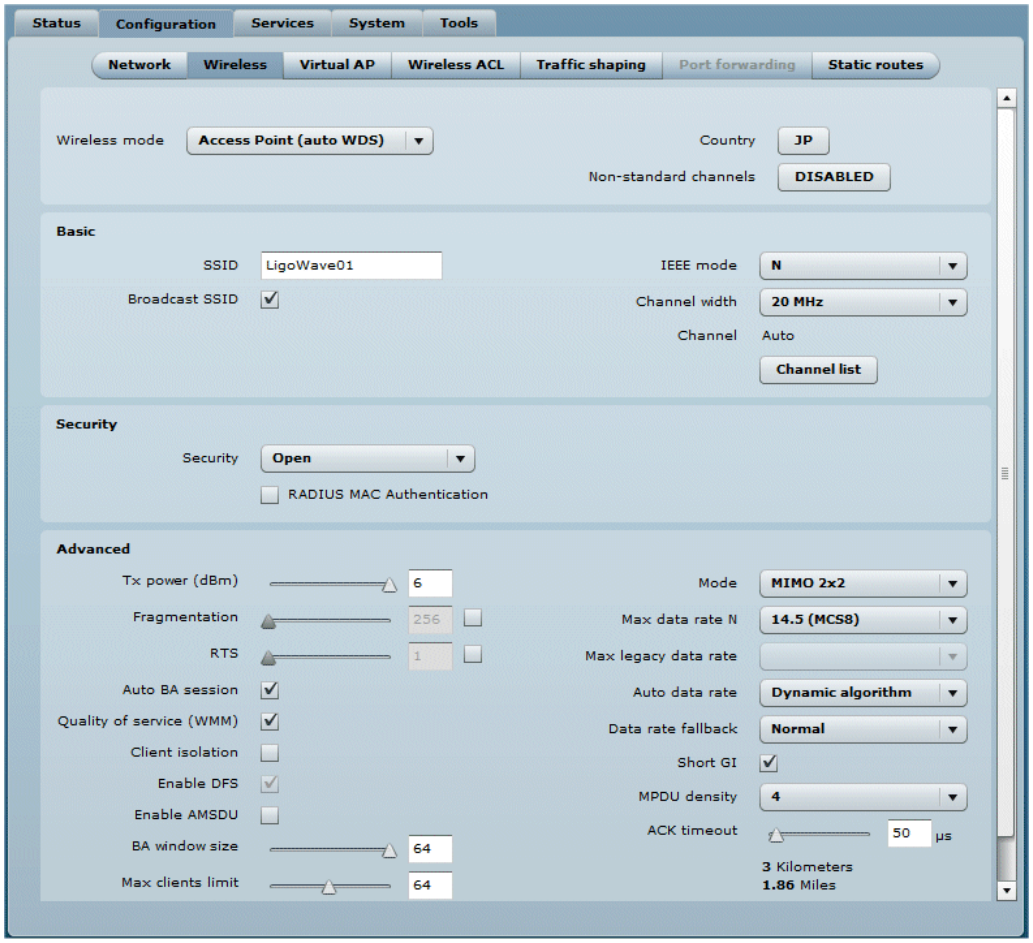
本装置の設定が適切であるかを確認してください。
設定が適切でないと接続ができません。
（たとえば、**Station(auto iPoll)**は **Access Point iPoll** としか接続できません。）

Country – “JP”(JAPAN)のみ設定可能です。


The correct country code must be selected before using the equipment to meet the regulatory requirements for authorized channels, channel width, output power, Dynamic Frequency Selection (DFS) and Automatic Transmit Power Control (ATPC). Installer or equipment owner takes all responsibility for proper product usage according to the regulatory rules. Vendor or distributor/reseller is not responsible for illegal wireless equipment operation. If you need any additional information, please send an email to support@deliberant.com.
I Agree
Operating country
JAPAN
JAPAN
OK
Cancel

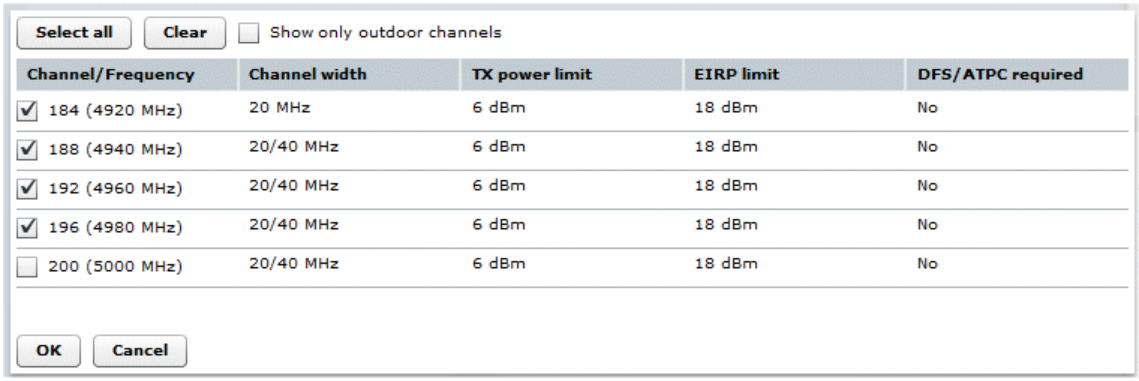
12.2.2.1. Access Point (auto WDS)

基本ワイヤレスを利用する本装置の無線インタフェースの設定

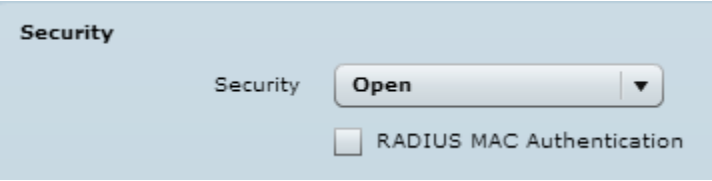


Access Point (auto WDS) – Basic 設定

項目	内容
SSID	本装置の SSID を設定します。
Broadcast SSID	アクセスポイントの SSID をブロードキャストするかどうかを設定します。
IEEE mode	wireless network モードを設定します。 A, A/N mixed, N
Channel width	帯域幅の設定を行います。
Channel	AP が動作しているチャンネルを表示します。 または、Auto Channel 機能が使用されていることを表示します。
Channel list	AP が動作するチャンネルを選択します。(複数可) 複数選択されると、オートチャンネル機能が有効になります。 AP は他の無線デバイスによって使用されていないチャンネルまたは、利用が少ないチャンネルを選択します。
Non-standard channels	この機能はサポートしていない為、使用しないでください。


Select all
Clear
Show only outdoor channels
Channel/Frequency
Channel width
TX power limit
EIRP limit
DFS/ATPC required
184 (4920 MHz) 20 MHz 6 dBm 18 dBm No
188 (4940 MHz) 20/40 MHz 6 dBm 18 dBm No
192 (4960 MHz) 20/40 MHz 6 dBm 18 dBm No
196 (4980 MHz) 20/40 MHz 6 dBm 18 dBm No
200 (5000 MHz) 20/40 MHz 6 dBm 18 dBm No
OK
Cancel

Access Point (auto WDS) – Security 設定

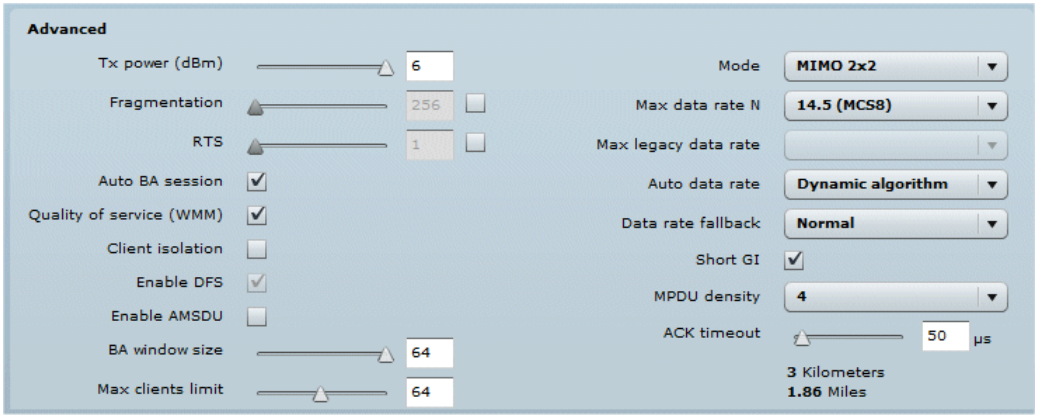


AP および Station のセキュリティ設定は同じ設定にしなければなりません。
装置には、さまざまな認証および暗号化の方法があります。

項目		内容
Security	Open	暗号化なし
	WEP	64bit または 128bit のWEP暗号化キーを使用します。
	Personal	暗号化方式として AES 或いは TKIP を使う pre-shared key 暗号化の WPA 規格または WPA2 規格です。
	Enterprise	RADIUS server での認証と AES または TKIP を使った WPA 規格/WPA2 規格の暗号化方式です。
RADIUS MAC Authentication	有効にすると、以下の項目が表示されます。	
	MAC format	MAC アドレス形式を選択します。
	RADIUS sever IP/ PORT	認証リクエストが転送される RASIUS server の IP アドレスとポート番号を設定します。 ポート番号の初期値は 1812 です。
	RADIUS key	認証サーバのセキュリティキーを設定します。 シークレットキーは、暗号化されたデータを RADIUS server と端末間で転送するためのものです。
	Override NAS ID	新しい NAS ID を入力します。

Access Point (auto WDS) - Advanced 設定

各種パラメータを設定することにより本装置の最高の性能を引き出すことができます。

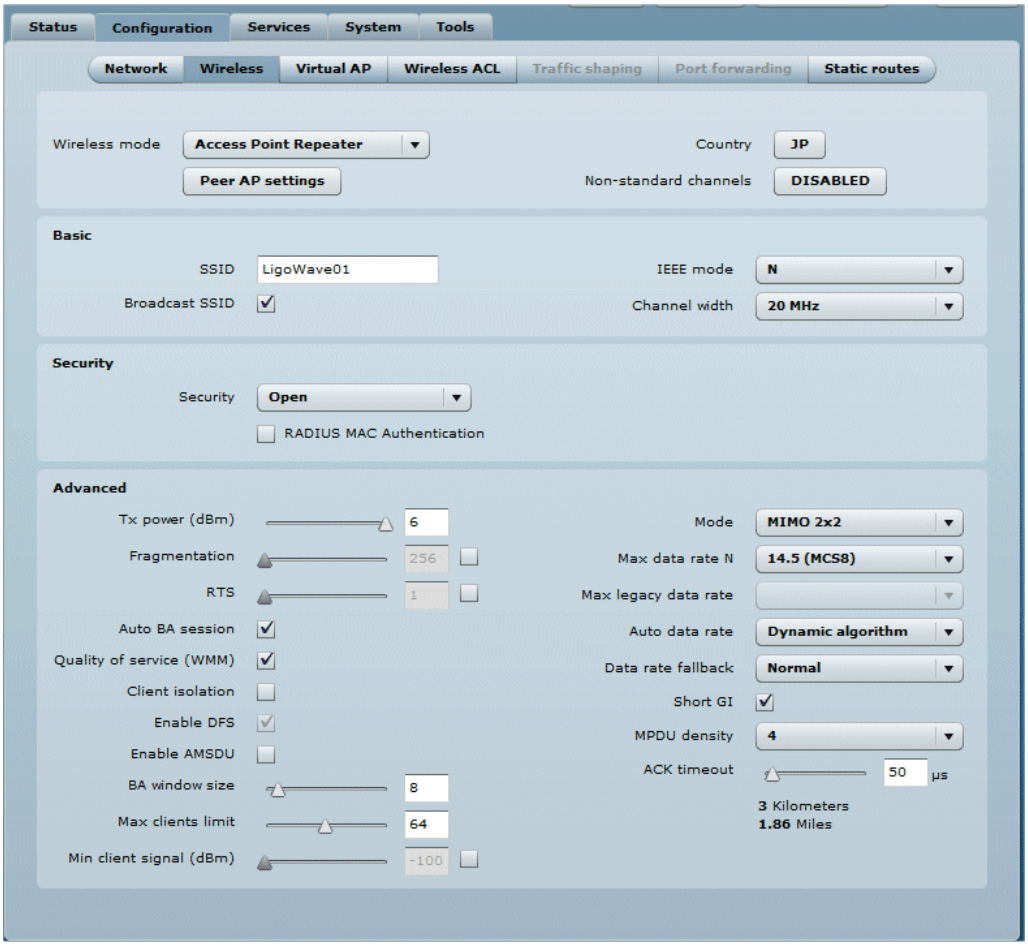


項目	内容
TX power	送信電力を設定します。送信距離が大きくなると大きな送信電力が必要になります。
Fragmentation	フラグメントの閾値を入力します[256-2346 bytes] この値は、データが複数のパケットに分割されて送信される前のパケットの最大値です。フラグメントの閾値があまりにも小さな値に設定されるとネットワークのパフォーマンスが下がります。この値については最小の変更が推奨されます。
RTS	RTS の閾値を入力します[0-2347 bytes]
Auto BA session	BA(ブロック ACK)の有効または無効の設定をします。
Quality of service(WMM)	トラフィックに優先度を付けるクオリティサービスを有効にします。
Client isolation	端末同士の通信を layer2 レベルで規制します。
Enable DFS	変更できません。
Enable AMSDU	AMSDU 機能を有効にするとパケットを連結し送信します。 802.11 モードの最大 MAC フレームサイズが大きくなります。
BA window size	BA(ブロック ACK)のウィンドウサイズを指定します。[1～64 まで]
Max clients limit	接続する無線クライアントの最大数を指定します。[1～127 まで]
Min clients limit(dBm)	有効にした場合、AP は、設定した値以下の信号を持っているクライアントとの接続を破棄します。[-100～-50dBm まで]

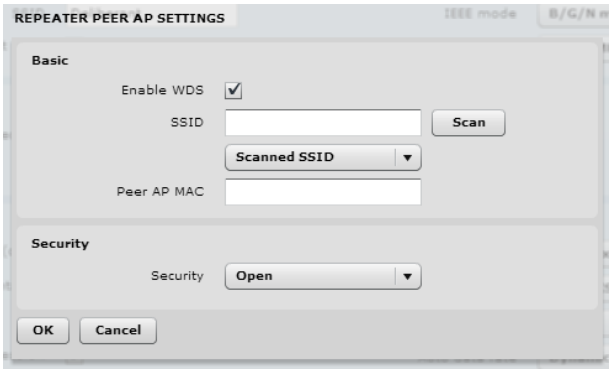
項目		内容
Mode	SISO 1x1	本装置は、1 つのアンテナのみをデータ転送に使います。
	MIMO 2x2	本装置は、2 つのアンテナを使いデータの転送をします。 （データ転送は同時に行われます。）
Max date rate N (IEEE802.11n)		パケットを転送する際の最大データレート[Mbps]を設定します。 最大データレートでデータを転送するように動作します。最大データレートでデータを転送できない場合、データレートを段階的に小さくしてデータを転送します。
Max legacy data rate (IEEE802.11a)		
Auto data rate		信号が低下した場合に、適切なデータレートを選択するアルゴリズムの選択をします。
	Fixed algorithm	指定された Max date rate N と Max legacy data rate でデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
	Dynamic algorithm	特定のアルゴリズムによって自動的に計算されたデータレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
Data rate fallback	Normal	最高のデータレートでデータ送信を開始し、最適なデータレートに到達するまで減少させます。
	Aggressive	Normal より安定化を重視するため、データレートを下げます。場合によっては MIMO から SISO への自動切り替えを行います。
Short GI		ショートガードインターバル機能を有効にします。 この機能が有効になると GI 値は 800ns から 400ns になります。
MPDU density		PPDU(PLCP Protocol Data Unit)間の最小時間を規定します。
ACK timeout		ACK timeout を規定します。 ACK timeout は、値を指定するか、link distance（通信距離）を指定することで自動入力されます。 ACK Timeout 値は、最大スループットのために最適値に合わせる必要があります。
Sensitivity/ Noise balance		感度とノイズのバランスを指定します。

12.2.2.2. Access Point Repeater

既存のネットワークインフラテクスチャの範囲を拡張するために使用します。



Peer AP settings



項目		内容
SSID		ペア AP の SSID を指定します。
	Scan	ワイヤレスネットワークの周囲をスキャンします。 見つかったネットワークの SSID は **Scanned SSID** で 利用できるようになります。
Peer Access Point MAC		ペア AP の MAC アドレスを入力します。Scanned SSID から選んだ場合は自動入力されます。
Security		選択したペア AP のセキュリティ設定を指定します。

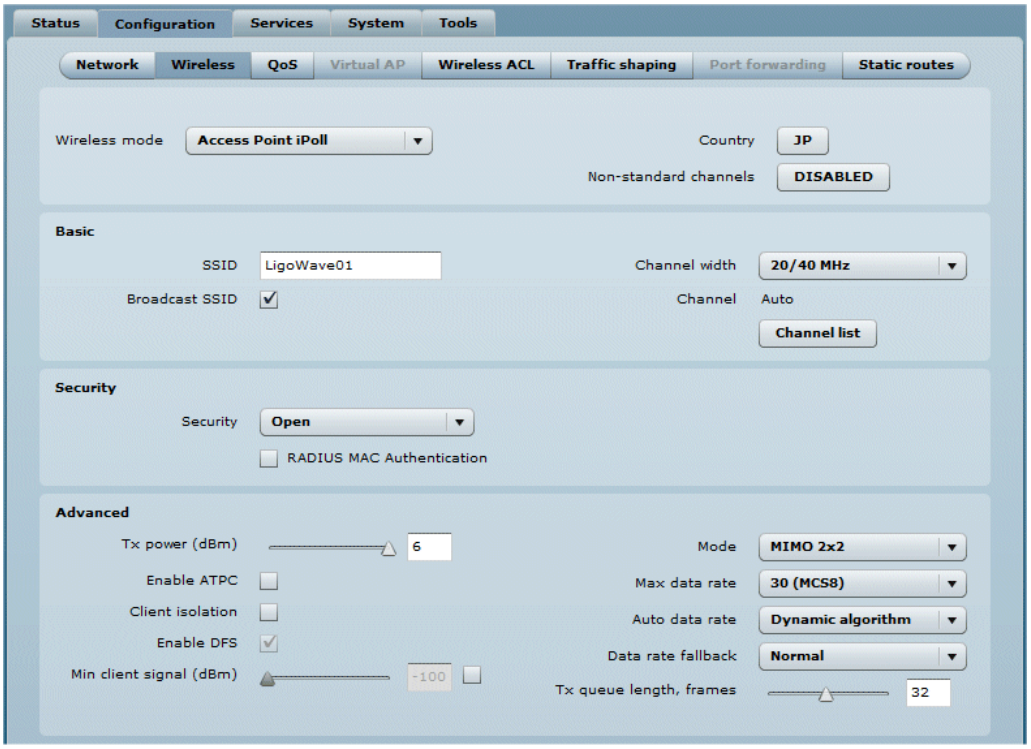
Access Point Repeater – Basic 設定
Access Point Repeater – Security 設定
Access Point Repeater – Advanced 設定

Basic、Security、Advanced 設定は、12.2.2.1 項 Access Point(auto WDS)と同様です。

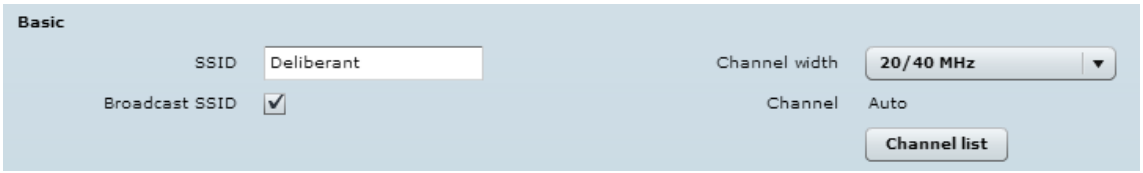
12.2.2.3. Access Point iPoll

iPoll wireless モードはポイントーマルチポイントワイヤレスソリューション用に設計されました。

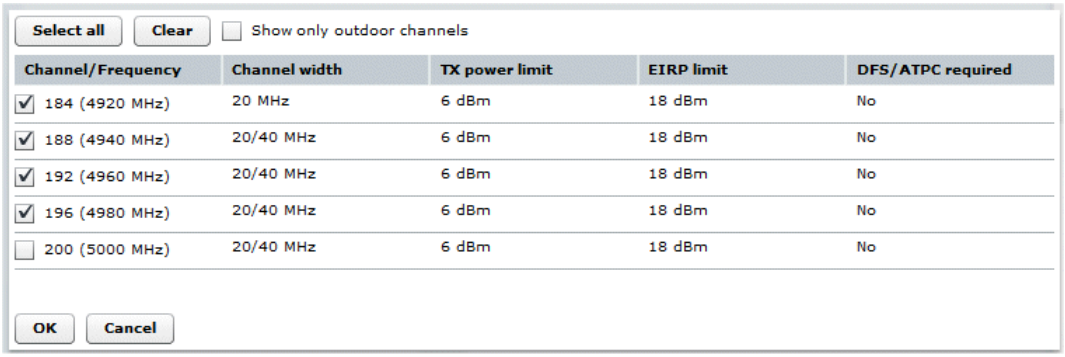
iPoll Access Point は、iPoll Station のみと接続し、信頼できるネットワークを構成します。



Access Point iPoll – Basic 設定



項目	内容
SSID	本装置の SSID を設定します。
Broadcast SSID	アクセスポイントの SSID をブロードキャストするかどうかを設定します。
Channel width	帯域幅の設定を行います。
Channel	AP が動作しているチャンネルを表示します。 または、Auto Channel 機能が使用されていることを表示します。
Channel list	AP が動作するチャンネルを選択します。(複数可) 複数選択されると、オートチャンネル機能が有効になります。 AP は他の無線デバイスによって使用されていないチャンネルまたは、利用が少ないチャンネルを選択します。

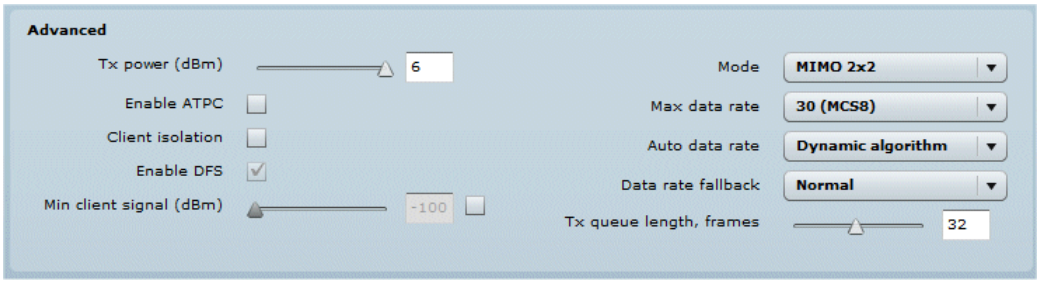


Access Point iPoll – Security 設定

Security 設定は、12.2.2.1 項　Access Point(auto WDS)と同様です。

Access Point iPoll – Advanced 設定

各種パラメータを設定することにより本装置の最高の性能を引き出すことができます。

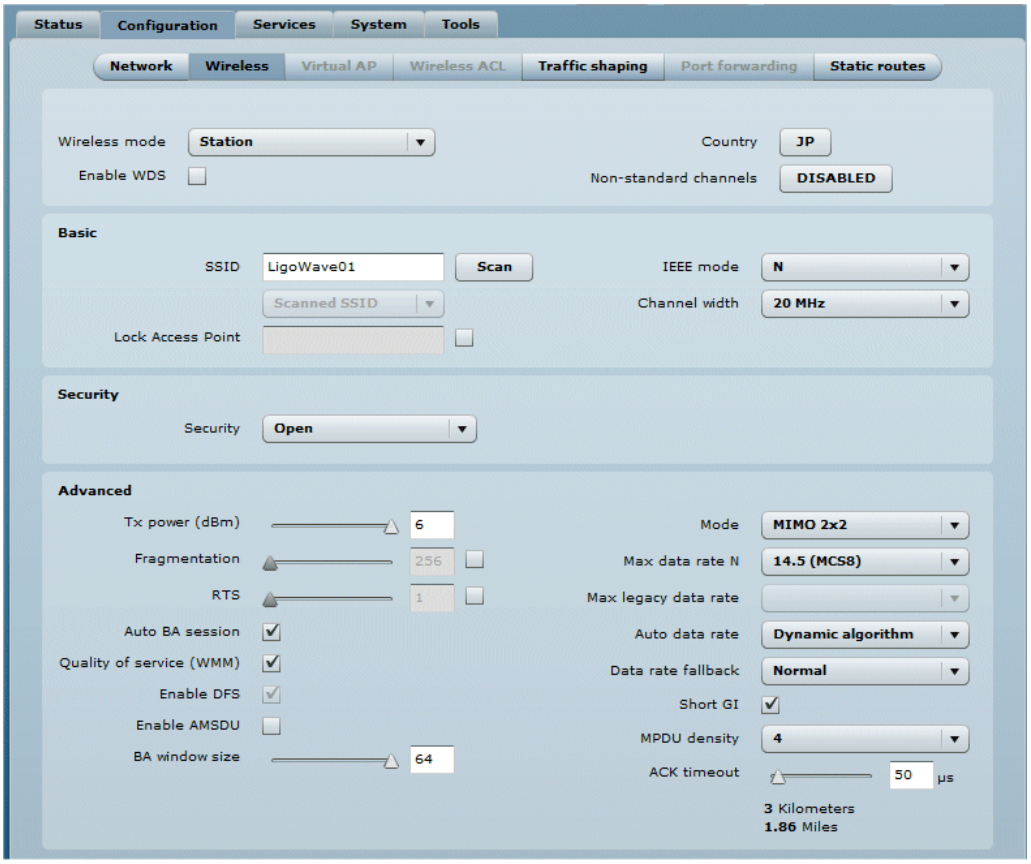


項目	内容
TX power	送信電力を設定します。送信距離が大きくなると大きな送信電力が必要になります。
Enable ATPC	ATPC（自動送信電力制御）を有効にします。
Client isolation	端末同士の通信を layer2 レベルで規制します。
Enable DFS	変更できません。
Min clients limit(dBm)	有効にした場合、AP は、設定した値以下の信号を持っているクライアントとの接続を破棄します。[−100～−50dBm まで]

項目		内容
Mode	SISO 1x1	本装置は、1 つのアンテナのみをデータ転送に使います。
	MIMO 2x2	本装置は、2 つのアンテナを使いデータの転送をします。 （データ転送は同時に行われます。）
Max date rate		パケットを転送する際の最大データレート[Mbps]を設定します。 最大データレートでデータを転送するように動作します。最大データレートでデータを転送できない場合、データレートを段階的に小さくしてデータを転送します。
Auto data rate		信号が低下した場合に、適切なデータレートを選択するアルゴリズムの選択をします。
	Fixed algorithm	指定されたレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
	Dynamic algorithm	特定のアルゴリズムによって自動的に計算されたデータレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
Data rate fallback	Normal	最高のデータレートでデータ送信を開始し、最適なデータレートに到達するまで減少させます。
	Aggressive	Normal より安定化を重視するため、データレートを下げます。場合によっては MIMO から SISO への自動切り替えを行います。
Tx queue length, frames		送信キューのフレーム長を指定します。
Sensitivity/ Noise balance		感度とノイズのバランスを指定します。

12.2.2.4. Station

Station 設定にすることで、無線クライアントとして動作します。

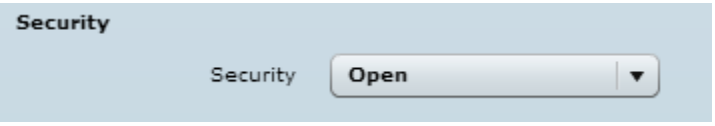


Station wireless の設定は、アクセスポイントの設定と少し異なります。
周囲にある SSID をスキャンし希望の AP を選択します。

Station- Basic 設定

項目	内容
SSID	本装置の SSID を設定します。
Scan	周囲の AP をスキャンします。ここで見つけた SSID はドロップダウンメニューに表示されます。
Scaned SSID	スキャンした SSID を表示します。
Channel	AP が動作しているチャンネルを表示します。 または、Auto Channel 機能が使用されていることを表示します。
Channel width	帯域幅の設定を行います。

Station- Security 設定

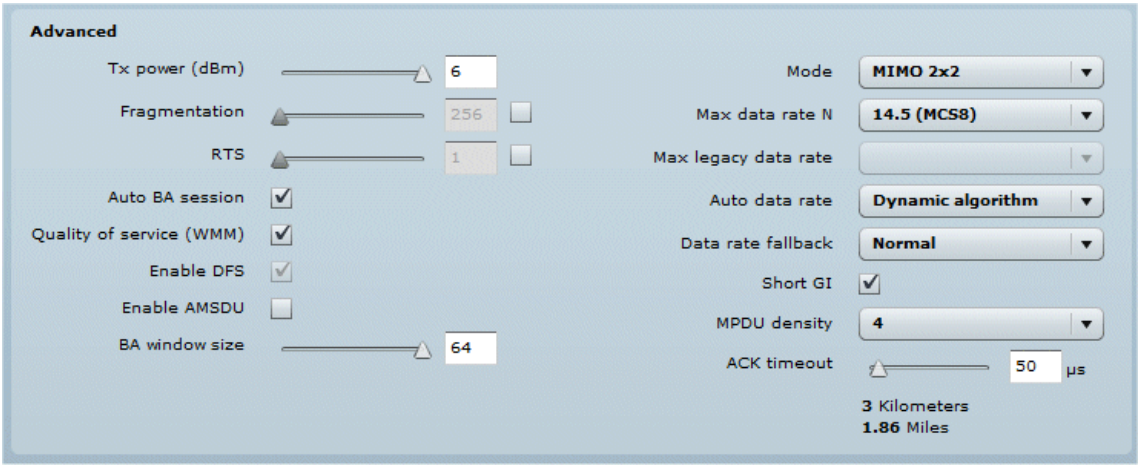


AP および Station のセキュリティ設定は同じ設定にしなければなりません。
装置には、さまざまな認証および暗号化の方法があります。

項目		内容
Security	Open	暗号化なし
	WEP	64bit または 128bit の WEP 暗号化キーを使用します。
	Personal	暗号化方式として AES 或いは TKIP を使う pre-shared key 暗号化の WPA 規格または WPA2 規格です。
	Enterprise	RADIUS server での認証と AES または TKIP を使った WPA 規格/WPA2 規格の暗号化方式です。

Station- Advanced 設定

各種パラメータを設定することにより本装置の最高の性能を引き出すことができます。

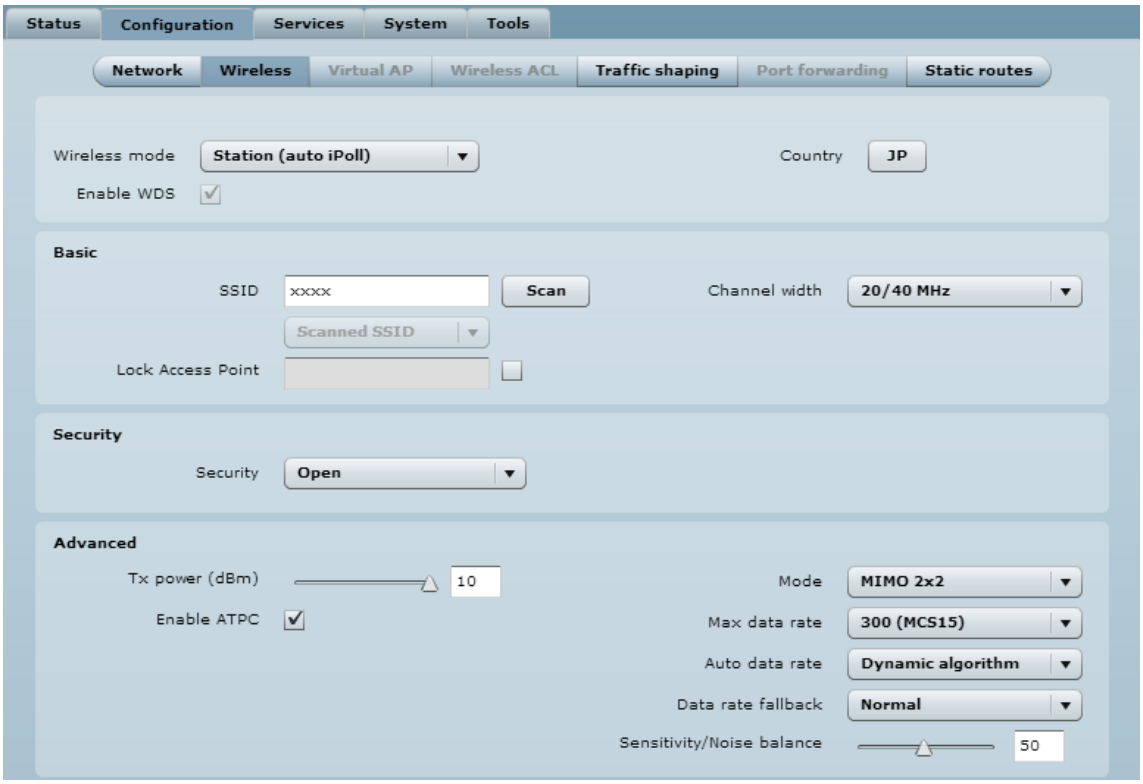


項目	内容
TX power	送信電力を設定します。送信距離が大きくなると大きな送信電力が必要になります。
Fragmentation	フラグメントの閾値を入力します[256-2346 bytes] この値は、データが複数のパケットに分割されて送信される前のパケットの最大値です。フラグメントの閾値があまりにも小さな値に設定されるとネットワークのパフォーマンスが下がります。この値については最小の変更が推奨されます。
RTS	RTS の閾値を入力します[0-2347 bytes]
Auto BA session	BA(ブロック ACK)の有効または無効の設定をします。
Quality of service(WMM)	トラフィックに優先度を付けるクオリティサービスを有効にします。
Client isolation	端末同士の通信を layer2 レベルで規制します。
Enable DFS	変更できません。(Propeller5 のみ)
Enable AMSDU	AMSDU 機能を有効にするとパケットを連結し送信します。 802.11 モードの最大 MAC フレームサイズが大きくなります。
BA window size	BA(ブロック ACK)のウィンドウサイズを指定します。[1～64 まで]

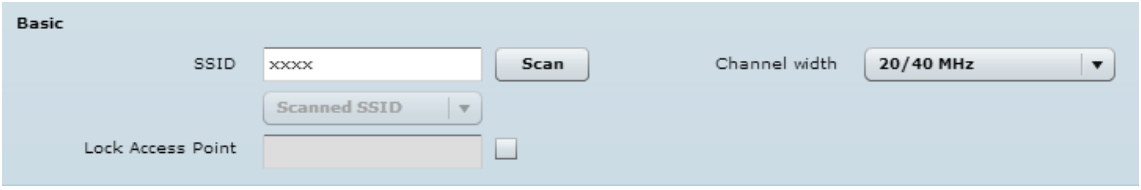
項目		内容
Mode	SISO 1x1	本装置は、1 つのアンテナのみをデータ転送に使います。
	MIMO 2x2	本装置は、2 つのアンテナを使いデータの転送をします。 （データ転送は同時に行われます。）
Max date rate N (IEEE802.11n)		パケットを転送する際の最大データレート[Mbps]を設定します。 最大データレートでデータを転送するように動作します。最大データレートでデータを転送できない場合、データレートを段階的に小さくしてデータを転送します。
Max legacy data rate (IEEE802.11a)		
Auto data rate		信号が低下した場合に、適切なデータレートを選択するアルゴリズムの選択をします。
	Fixed algorithm	指定された Max date rate N と Max legacy data rate でデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
	Dynamic algorithm	特定のアルゴリズムによって自動的に計算されたデータレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
Data rate fallback	Normal	最高のデータレートでデータ送信を開始し、最適なデータレートに到達するまで減少させます。
	Aggressive	Normal より安定化を重視するため、データレートを下げます。場合によっては MIMO から SISO への自動切り替えを行います。
Short GI		ショートガードインターバル機能を有効にします。 この機能が有効になると GI 値は 800ns から 400ns になります。
MPDU density		PPDU(PLCP Protocol Data Unit)間の最小時間を規定します。
ACK timeout		ACK timeout を規定します。 ACK timeout は、値を指定するか、link distance（通信距離）を指定することで自動入力されます。 ACK Timeout 値は、最大スループットのために最適値に合わせる必要があります。

12.2.2.5. Station（auto iPoll）

Station(auto iPoll)に設定にすることで、Access Point iPoll 専用の無線クライアントとして動作します。

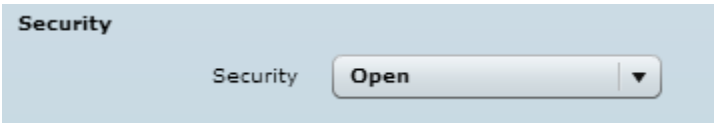


Station(auto iPoll) – Basic 設定



項目	内容
SSID	本装置の SSID を設定します。
Scan	周囲の AP をスキャンします。ここで見つけた SSID はドロップダウンメニューに表示されます。
Scaned SSID	スキャンした SSID を表示します。
Channel width	帯域幅の設定を行います。

Station(auto iPoll) – Security 設定

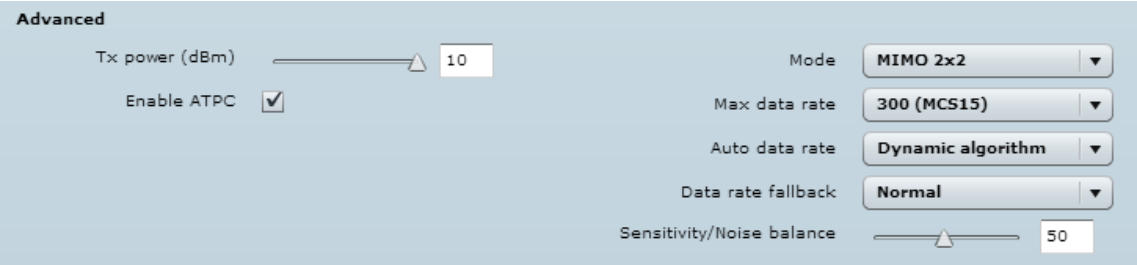


AP および Station のセキュリティ設定は同じ設定にしなければなりません。
装置には、さまざまな認証および暗号化の方法があります。

項目		内容
Security	Open	暗号化なし
	WEP	64bit または 128bit の WEP 暗号化キーを使用します。
	Personal	暗号化方式として AES 或いは TKIP を使う pre-shared key 暗号化の WPA 規格または WPA2 規格です。
	Enterprise	RADIUS server での認証と AES または TKIP を使った WPA 規格/WPA2 規格の暗号化方式です。

Station(auto iPoll) – Advanced 設定

各種パラメータを設定することにより本装置の最高の性能を引き出すことができます。

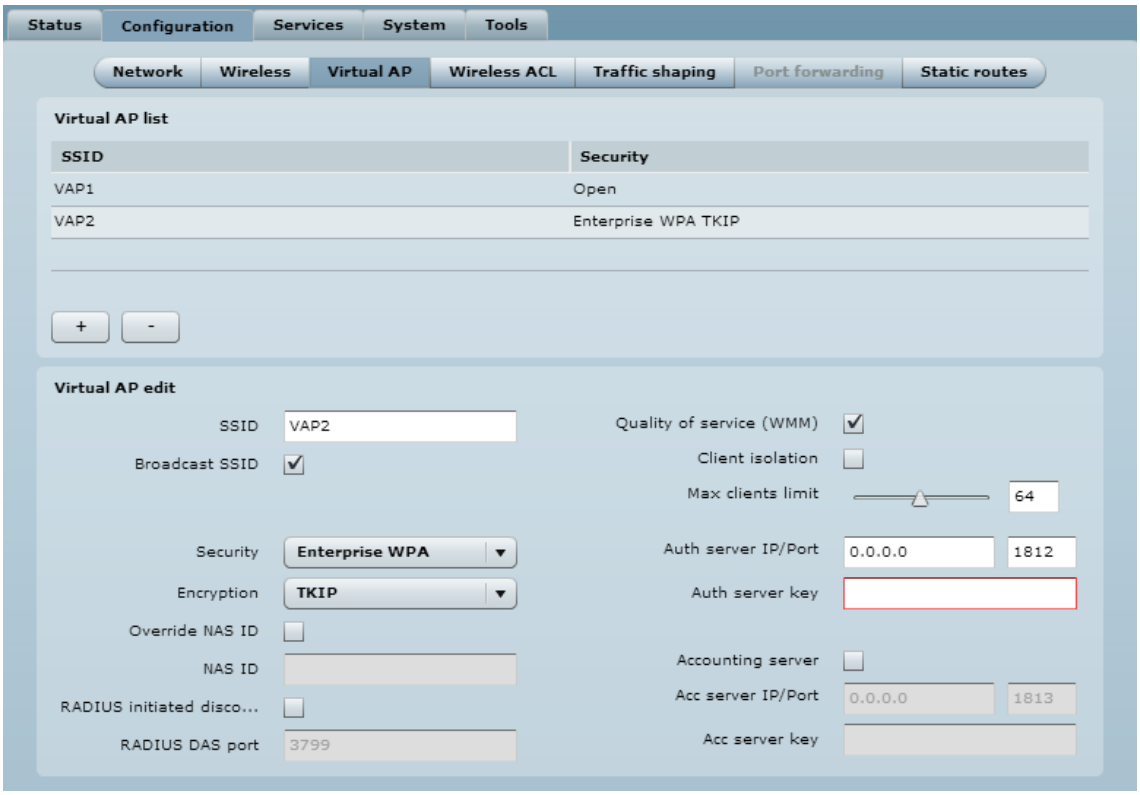


項目		内容
TX power		送信電力を設定します。送信距離が大きくなると大きな送信電力が必要になります。
Enable ATPC		ATPC(自動送信電力制御)を有効にします。
Client isolation		端末同士の通信を layer2 レベルで規制します。
Enable DFS		変更できません。
Min clients limit(dBm)		有効にした場合、AP は、設定した値以下の信号を持っているクライアントとの接続を破棄します。[-100～-50dBm まで]
Mode	SISO 1x1	本装置は、1 つのアンテナのみをデータ転送に使います。
	MIMO 2x2	本装置は、2 つのアンテナを使いデータの転送をします。 (データ転送は同時に行われます。)
Max date rate		パケットを転送する際の最大データレート[Mbps]を設定します。 最大データレートでデータを転送するように動作します。最大データレートでデータを転送できない場合、データレートを段階的に小さくしてデータを転送します。
Auto data rate		信号が低下した場合に、適切なデータレートを選択するアルゴリズムの選択をします。
	Fixed algorithm	指定されたレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
	Dynamic algorithm	特定のアルゴリズムによって自動的に計算されたデータレートでデータの送信を開始し、最適なデータレートに到達するまで徐々にステップダウンします。
Data rate fallback	Normal	最高のデータレートでデータ送信を開始し、最適なデータレートに到達するまで減少させます。
	Aggressive	Normal より安定化を重視するため、データレートを下げます。場合によっては MIMO から SISO への自動切り替えを行います。
Sensitivity/ Noise balance		感度とノイズのバランスを指定します。

12.2.3. Virtual AP

Virtual AP 機能は、**Access Point (auto WDS)**モードと
Access Point Repeater モードのみで動作します。

最大 3 個※まで Virtual AP を追加設定することができます。Virtual AP は、論理的なワイヤレスネットワークであり、本装置は、設定した 3 個の wireless network 毎に radio interface を設定することができます。全ての Virtual AP は同時に動作し client 端末は任意の Virtual AP に接続することができます。



新しい Virtual AP を定義するには＋ボタンをクリックし新しいエントリーを VAP テーブルに作成します。そして、作成したエントリーを選択し必要な設定を行います。

※4 個以上設定できますが、動作保証できません。

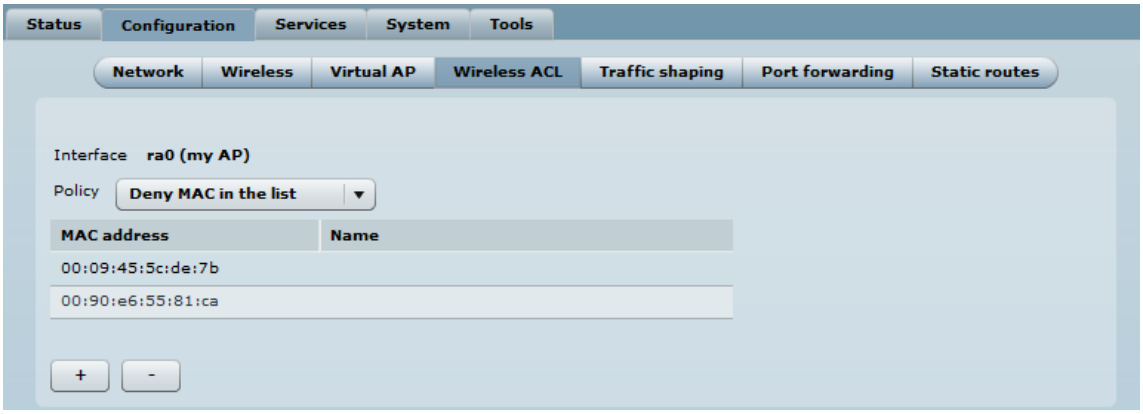
Virtual AP edit

項目		内容
SSID		本装置の SSID を設定します。
Broadcast SSID		アクセスポイントの SSID をブロードキャストするかどうかを設定します。
Quality of service(WMM)		トラフィックに優先度を付けるクオリティサービスを有効にします。
Client isolation		端末同士の通信を layer2 レベルで規制します。
Max client limit		接続する無線クライアントの最大数を指定します。[1～127 まで]
Security	Open	暗号化なし
	WEP	64bit または 128bit の WEP 暗号化キーを使用します。
	Personal	暗号化方式として AES 或いは TKIP を使う pre-shared key 暗号化の WPA 規格または WPA2 規格です。
	Enterprise	RADIUS server での認証と AES または TKIP を使った WPA 規格/WPA2 規格の暗号化方式です。

Wireless client は、特定のセキュリティ構成で応答することができなければなりません。

12.2.4. Wireless ACL

Wireless ACL 機能は、**Access Point (auto WDS)**モードと
Access Point Repeater モードと **Access Point iPoll** モードのみで動作します。



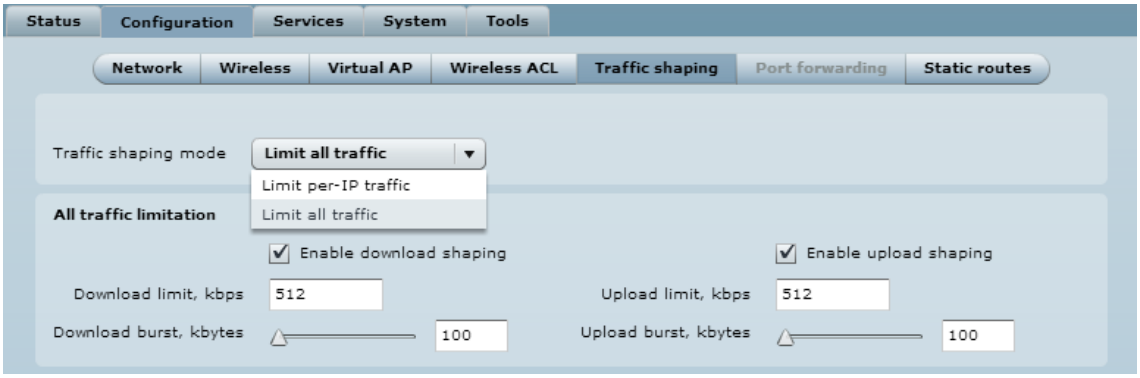
項目		内容
Security	Open	暗号化なし
	Allow MAC in the list	list にある MAC アドレスのみが AP と接続できます。
	Derry MAC in the list	list にある MAC アドレスのみが AP と接続できません。

新しいルールを追加するには、「+」ボタンを押してください。
削除するには、削除したいルールを選択し「−」ボタンを押してください。
フィールド上のルールをクリックすると編集できます。

12.2.5. Traffic Shaping

Traffic Shaping 機能は、**Access Point Repeater** モードでは、使用できません。

ダウンロードあるいはアップロードのトラフィック(通信量)を制御し、通信性能を最適化/保証するために Traffic Shaping を設定します。2つのトラフィックを制御方法があります。



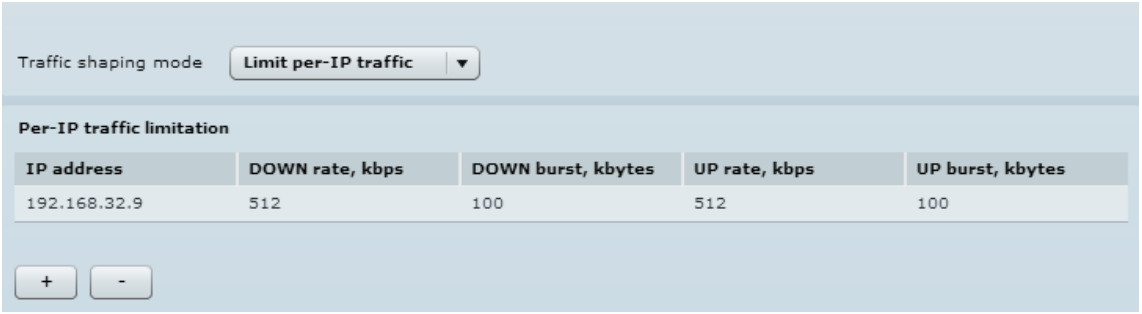
項目	内容
Limit all traffic	本装置からアップロードする全ての通信量と、本装置にダウンロードする全ての通信量を制限します。
Limit per IP traffic	本装置からアップロードする通信量と本装置にダウンロードする通信量を、限定した IP アドレスにより制限します。

Traffic shaping mode – Limit all traffic

項目		内容
Enable download shaping		ダウンロード通信量の制限を有効にします。
	Download Limit, kbps	最大ダウンロード(wireless interface から Ethernet interface へ)帯域の値を Kbps で設定します。
	Download burst, kbytes	ダウンロードバーストサイズを kbyte で設定します。
Enable upload shaping		アップロード通信量の制限を有効にします。
	Upload limit, kbps	最大アップロード(Ethernet interface から wireless interface へ)帯域の値を Kbps で設定します。
	Upload burst, kbytes	アップロードバーストサイズを kbyte で 設定します。

Traffic shaping mode – Limit per IP traffic

「+」ボタンをクリックして新しいトラフィック制限ルールを作成します。



項目	内容
IP address	制限するトラフィックの IP アドレスを設定します。
Down rate, kbps	最大ダウンロード（wireless interface から Ethernet interface へ）の帯域を kbps で設定します。
Down burst, kbytes	ダウンロードバーストサイズを kbyte で設定します。
UP rate, kbps	最大アップロード（Ethernet interface から wireless interface へ）の帯域を kbps で設定します。
Down rate, kbytes	アップロードバーストサイズを kbyte で設定します。

12.2.6. Port Forwarding

Port forwarding 機能は、**Router** network mode のみで使える機能です。
NAT 機能が有効になっている場合にのみ Port Forwarding,
UPnP および DMZ が有効になります。

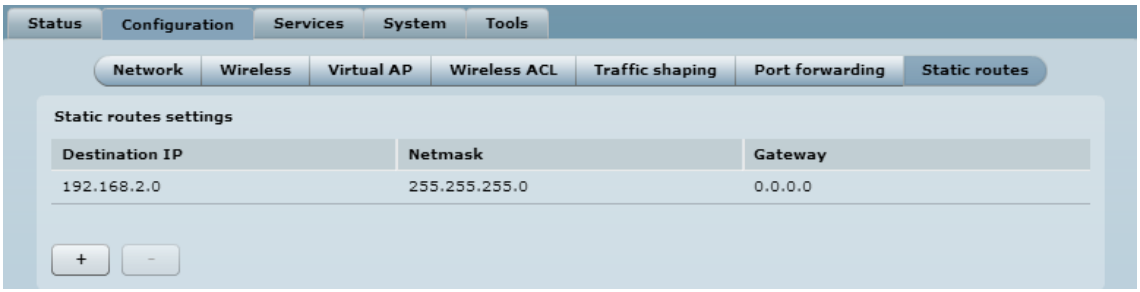
Port forwarding は、NAT 機能が有効なときトラフィックを LAN 側へ通過させます。例えば、本装置が router mode で NAT 機能が有効なとき、WAN interface の外にある端末から LAN 側に設置した端末のプライベート IP アドレスは分かりません。Port forwarding 機能あるいは DMZ を設定することによりトラフィックをプライベート IP アドレスへ通過させることができます。

項目	内容
Enable UPnP	UPnP 機能を有効にします。 本装置が他のネットワーク機器と自動的に必要なポートを解放し ネットワーク機器と接続することを可能にします。
Enable DMZ	DMZ 機能を有効にします。 特定の IP アドレスに対して全ての TCP/UDP ポートを解放し、 本装置にサーバを接続することを可能にします。 一般に VoIP やマルチメディアサーバに利用されます。
Public port	public IP アドレスで利用されるポートを設定します。
Private host	トラフィックをフォーワードする NAT の配下にある端末の IP アドレスを設定します。
Private port	NAT の配下にありトラフィックを受け取る端末のポートを設定します。
Protocol	TCP または UDP を設定します。

12.2.7. Static Routes

Static routes は、**Router** network mode のみで使える機能です。

ルーティングルールは、トラフィックの送り先のインタフェースまたはゲートウェイの IP アドレスおよびネットマスクによって定義されます。データパケットは、指定されたルータインタフェースあるいは他のゲートウイルータへ送られます。
新しいスタティックルートを設定するには次のパラメータを設定します。

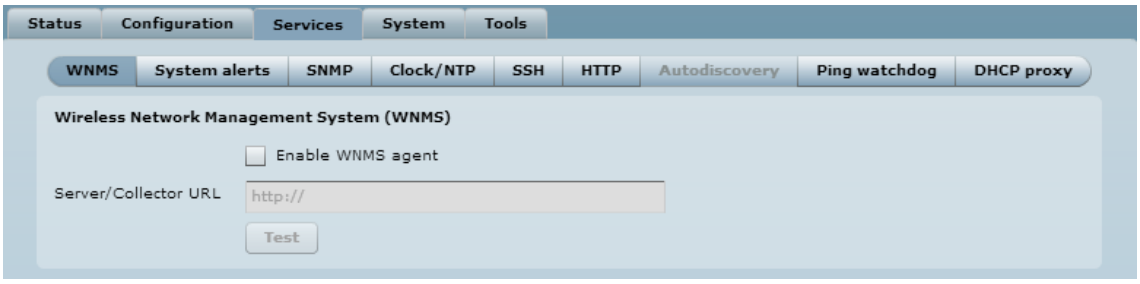


項目	内容
Destination IP	トラフィックの送り先 IP アドレスを設定します。
Netmask	トラフィックの送り先ネットマスクを設定します。
Gateway	ゲートウェイアドレスを設定します。ゲートウェイの初期値は、0.0.0.0 です。

12.3. Services

12.3.1. WNMS

Wireless Network Management System(WNMS)は、集中型のモニタリングおよびマネジメントシステムです。WNMSと管理対象の装置の通信は、WNMS serviceを持つ装置から開始されます。



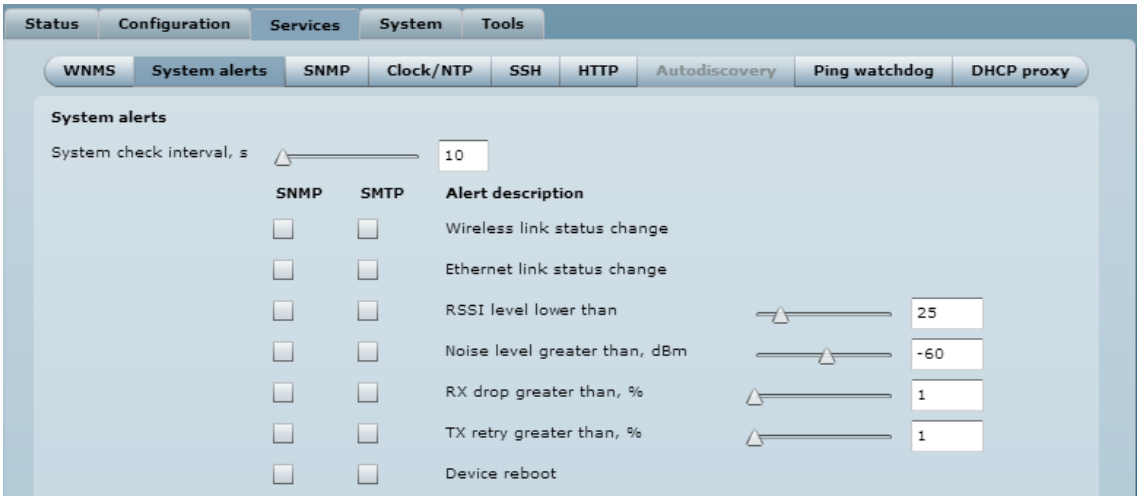
項目	内容
Enable WNMS agent	WNMS 機能を有効にします。
Server/Collector URL	heartbeat 情報を受信する WMS server の URL を設定します。
Test	指定されたサーバの応答が成功したかどうかのチェックをします。

12.3.2. System alerts

システムにエラーが発生したとき装置はエラーのアラートを外部に転送することができます。

Alert は、SNMP Traps または SMTP notifications として転送されます。

SNMP Traps と SMTP notifications は、同時に利用することもできます。



項目	内容
System alerts	システムの alert notification 機能を選択して有効にします。
System check interval, s	予期しないシステムの異常が発生した場合、本装置が alert notification を送信する時間間隔を秒単位で設定します。
Wireless link status change	システムは、Wireless link の状態が変化した場合、警報を送ります。
Ethernet link status change	システムは、Ethernet link の状態が変化した場合、警報を送ります。
RSSI level lower than	システムは、RSSI レベルが設定値よりも小さくなった場合、警報を送ります。初期値は 25 です。
Noise level greater than	システムは、signal noise レベルが設定値より大きくなった場合、警報を送ります。初期値は-60 dBm です。
RX drop greater than	システムは、RX のパケット落ちが設定したパーセンテージよりも多き場合、警報を送ります。初期値は 250 パケット/秒です。
TX retry greater than	システムは、TX のパケット落ちが設定したパーセンテージよりも多き場合、警報を送ります。初期値は 250 パケット/秒です。
Device reboot	システムは、本装置が予期せずリブートしたとき、あるいは管理者が本装置をリブートした場合、警報を送ります。

SNMP Trap Settings

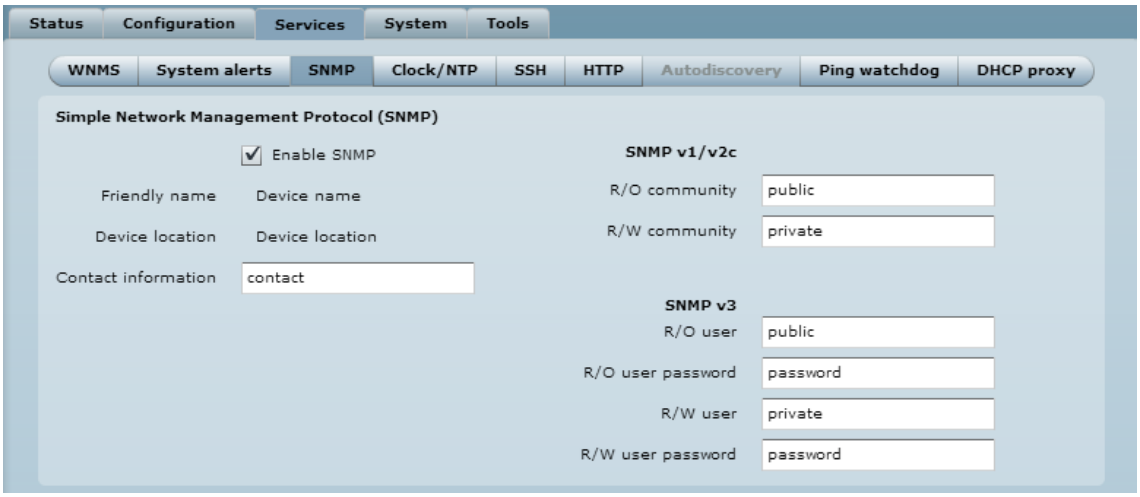
項目	内容
Manager address	SNMP Trap receiver の IP アドレスまたは hostname を設定します。
Manager port	Trap server のポート番号を設定します。 初期値:162
Trap community	SNMP community の文字列を設定します。 この文字列は、SNMP manager と本装置のパスワードになります。 初期値:public
Use inform	警報を受信したとき SNMP manager からのリトライ設定を行います。
Retry count	リトライ回数を設定します[1-10] 初期値:5
Retry timeout	警報を再送するリクエスト送る前に Trap server から送られてくる応答をどれくらいの時間待つかを秒単位設定します[1-10] 初期値:1

SMTP Setting

項目	内容
Server address	SMTP server の IP アドレスまたは hostname を設定します。
Server port	SMTP server のポート番号を設定します。初期値:25
Source e-mail address	本装置で使うメールアドレスを設定します。
Destination e-mail address	送り先のメールアドレスを設定します。
E-mail notification interval	警報情報を送信する間隔を秒単位で設定します[0-86400] 0 に設定されるとシステムに異常が発生した場合、警報情報は直ちに送信されます。
Username	SMTP サーバにアクセスするのに必要なユーザ名を入力します。
Password	SMTP サーバにアクセスするのに必要なパスワードを入力します。
Encryption	SMTP 認証の暗号化方式を TLS1.0 か SSL3.0 で選択します。

12.3.3. SNMP

SNMP 機能が有効になると本装置は、SNMP agent をして作動します。



項目	内容
Enable SNMP	SNMP service 機能を有効にします。
Friendly name	本装置の名前を表示します。 この名前は、Device settings で設定した Friendly name です。
Link location	本装置の設置場所を表示します。 この場所は、Device settings で設定した場所です。
Contact information	本装置を管理する管理者や管理者への連絡方法等を入力します

SNMP v1/v2c

項目	内容
R/O community	Read-only コミュニティの設定を行います。Read-only コミュニティのマネージャは情報を読むことはできますが情報を変更することはできません。
R/W community	Read-Write コミュニティを設定します。Read-Write コミュニティのマネージャは読み取りの値を変更できます。

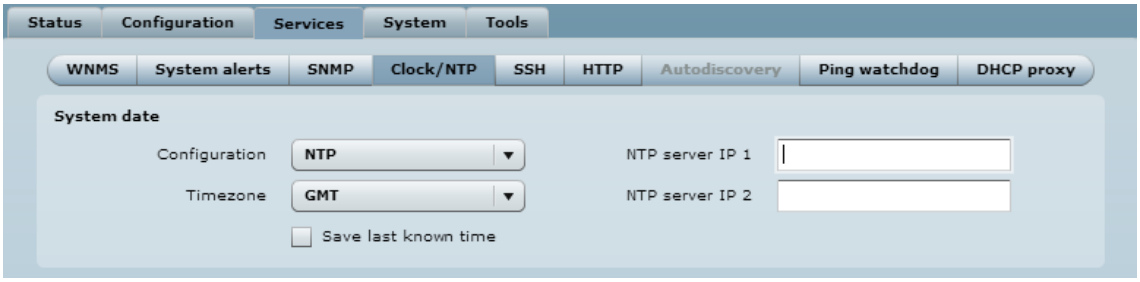
SNMP v3

項目	内容
R/O user	Read-only SNMPv3 でアクセスするユーザ名を設定します。 Read-only コミュニティのマネージャは情報を読むことはできますが変更することはできません。
R/O user password	Read-only SNMPv3 でアクセスするためのパスワードを設定します。
R/W user	Read- write SNMPv3 でアクセスするユーザ名を設定します。 Read-write コミュニティのマネージャは情報を読むができ、変更もすることができます。
R/W user password	Read- write SNMPv3 でアクセスするためのパスワードを設定します。

12.3.4. Clock/NTP

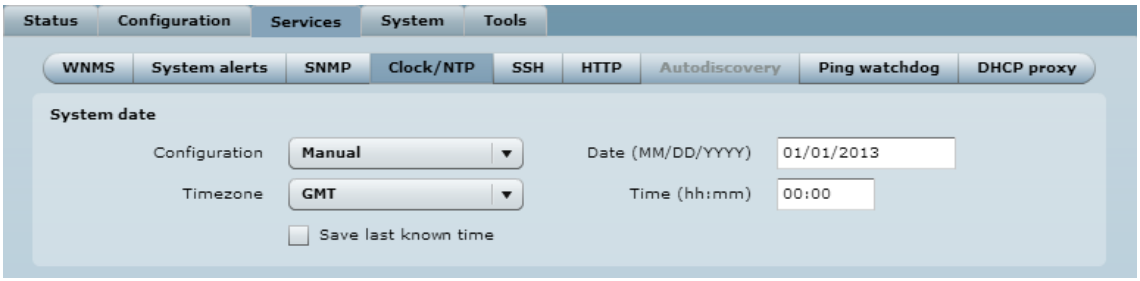
このセクションでシステムの時間および日付を制御します。NTP(Network Time Protocol)を使うかマニュアルで設定します。NTP client は、定義された time server に同期します。

NTP を使用する場合、configuration メニューから NTP を選択し、location time zone および NTP server を設定します。



項目	内容
Configuration	system clock のモードを NTP に設定します。
Time zone	Time zone を設定します。 Time zone は、local time と GMT の差で設定します。
Save last known time	本設定を有効にすることにより最後にリブートした時間を再現します。NTP が有効な時、NTP サーバが利用できない場合、最後にリブートした時間を設定します。
NTP server	信頼性のある NTP server IP アドレスまたは hostname を設定します。

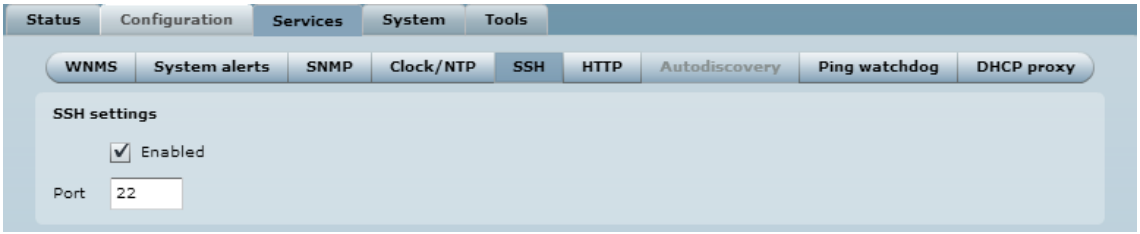
Clock をマニュアルで調整する場合、configuration モードを Manual にし、以下の設定を行います。



項目	内容
Configuration	system clock のモードを Manual に設定します。
Time zone	Time zone を設定します。 Time zone は、local time と GMT の差で設定します。
Date	新しい日付を MM/DD/YYYY のフォーマットで設定します。
Time	時間を hh:mm のフォーマットで設定します。

12.3.5. SSH

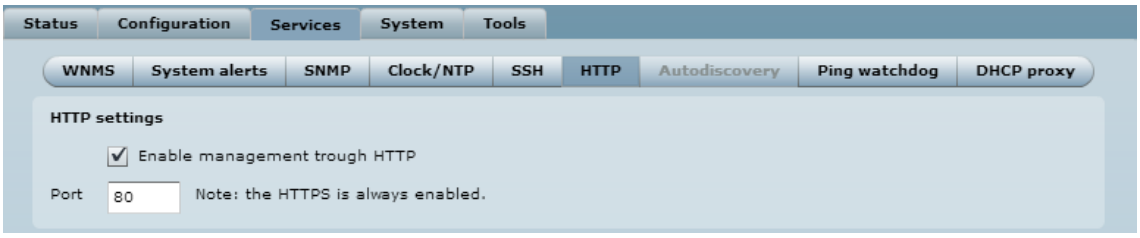
装置へ SSH プロトコルでアクセスするための制御を行います。



項目	内容
Enabled	本装置に対して SSH によるアクセスを有効にします。
Port	SSH service のポート番号を設定します。初期値：22

12.3.6. HTTP

本装置に web management interface でアクセスするための HTTP にかかわる設定を行います。



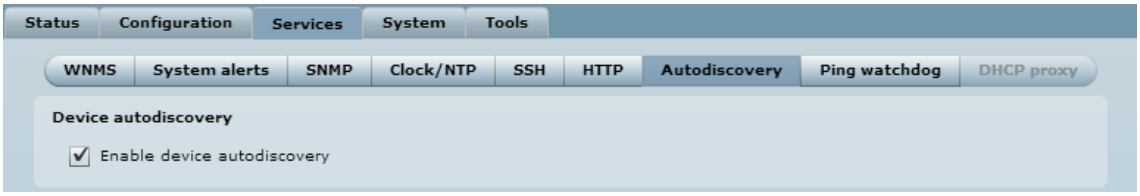
項目	内容
Enable management through HTTP	HTTP access を有効にします。
Port	HTTP のポート番号を設定します。 標準の HTTP ポート番号は 80 です。

HTTPS 接続の標準ポート番号 8080 も利用可能です。

12.3.7. Auto discovery

Auto discovery 機能は、station モードと station(Auto iPoll)モードでのみ使用できます。

有効にすると、単一のマルチキャストパケットの届く範囲のユニットの検出を可能にします。

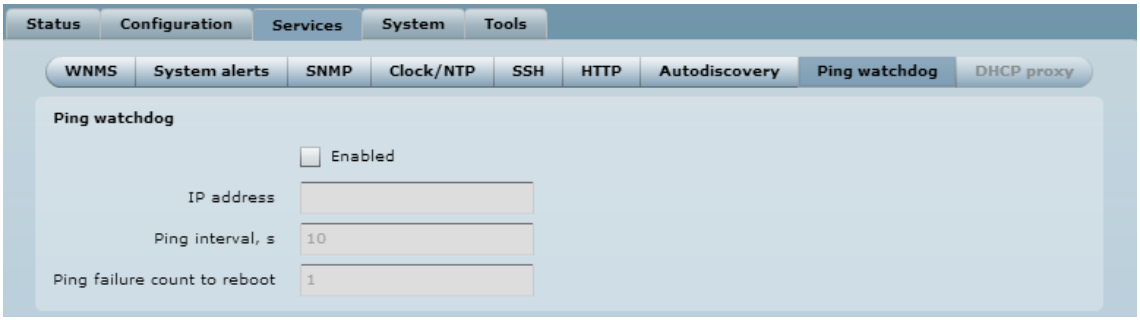


項目	内容
Enable device auto discovery	自動検出機能を有効にします。

12.3.8. Ping watching

有効にすると、指定されたホストと本装置のネットワーク接続の継続的な監視をします。

有効にした場合、本装置は指定されたホストに定期的に Ping 要求を送信します。時間内に応答がない場合、本装置を再起動します。



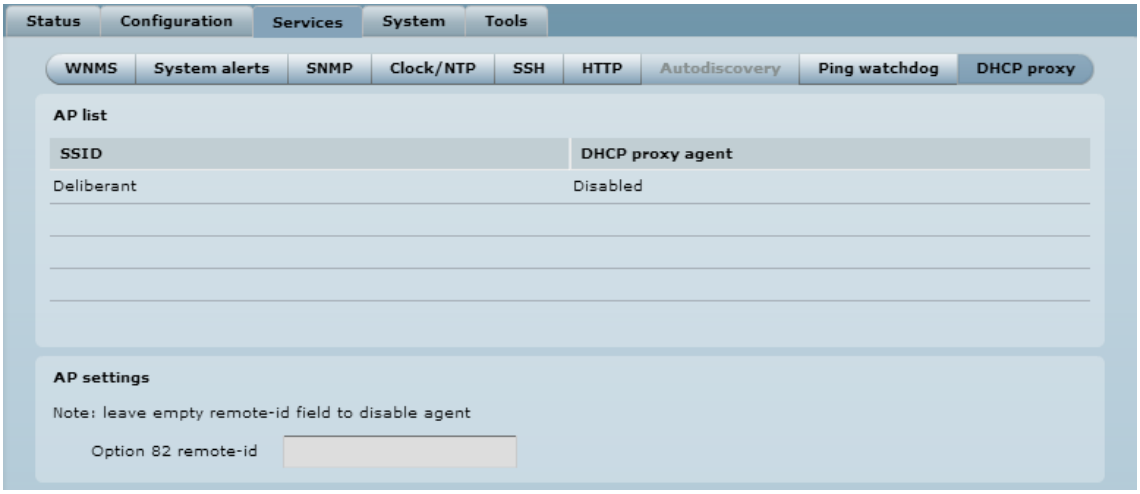
項目	内容
Enable	Ping のウォッチドッグ機能を有効にします。
IP address	Ping リクエストが送信されるホストを指定します。
Ping interval	Ping リクエストの間隔を秒単位で指定します。
Ping failure count to reboot	Ping の再送カウントを指定します。 指定した回数 Ping 監視に失敗した場合、本装置は自身を再起動します。

12.3.9. DHCP proxy

DHCP Proxy 機能は、**Access Point** または **Access Point Repeater** モードで、**Bridged** 動作する場合のみ使用できます。

DHCP オプション 82 は、信頼できないソースからの DHCP クライアント要求を防止するために、AP が DHCP リレーエージェントとして機能を有効にします。

AP リストに必要な SSID を選択し、AP の設定は DHCP プロキシを有効できるようになります。



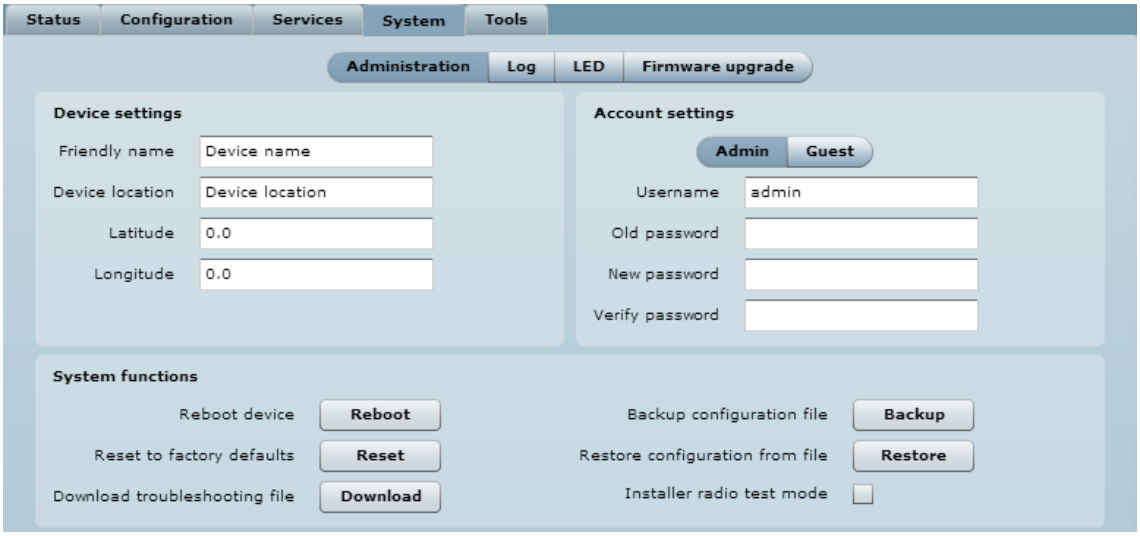
項目	内容
Option 82 remote-id	DHCP サーバが DHCP プロキシ要求を受け入れるための リモート ID を指定します。

12.4. System

12.4.1. Administration

セキュリティの観点から初期値の administrator username および password については変更されることを推奨しています。

System メニューではメインシステムを制御する設定を行います。また、本装置のリブート、設定の再インストールなどを行うことができます。このメニューは 3 つのパートに分かれています。Device stings、Account settings および system functions です。



Device settings

項目	内容
Friendly name	本装置の名前を入力します。
Device location	本装置の設置場所を入力します[最大 255 の ASCII キャラクタ]。
Longitude	本装置の設置されている経度を入力します。 [10 進数で入力します。例えば 54.869446]
Latitude	本装置の設置されている緯度を入力します。 [10 進数で入力します。例えば 23.891058]

Account settings

Administrative Account メニューで管理者のパスワードを変更することができます。

初期の管理者ログイン設定は以下のとおりです。

Username: admin

Password: admin01

項目	内容
User name	ユーザ名を変更します。
Old password	古い password を入力します。
New password	新しい password を入力します。
Verify password	確認のために再度新しい password を入力します。

本装置に web management interface でアクセスする場合、password を忘れた場合は、工場出荷状態に戻す必要があります。

System functions

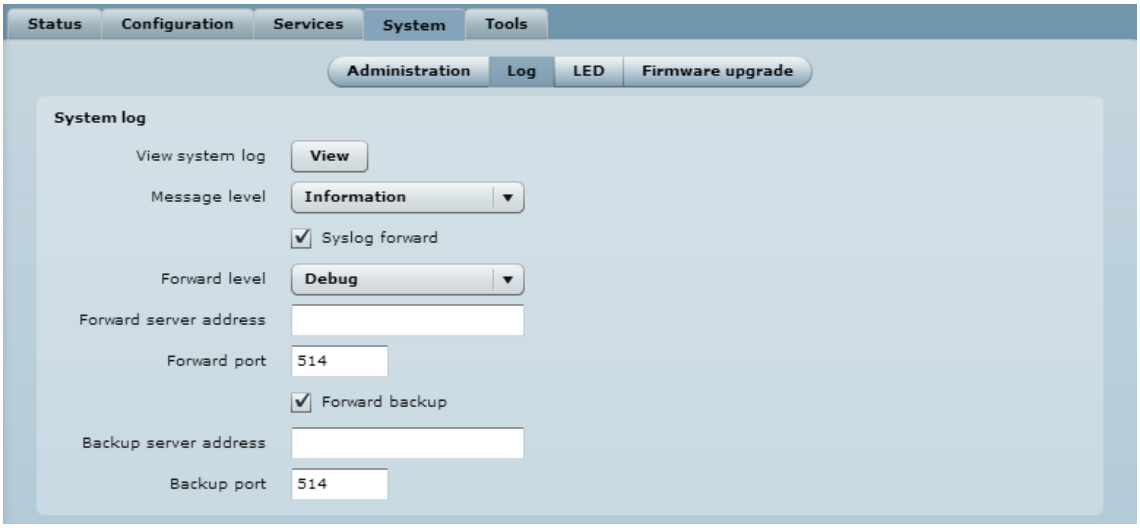
本装置のリセット処理は取り消すことができません。現在の設定および password は工場出荷時の状態に戻ります。

項目	内容
Reboot device	最後に Save した設定でリブートします。
Reset device to factory defaults	本装置を工場出荷時の状態に戻します。
Download troubleshooting file	troubleshooting file をダウンロードします。 troubleshooting file には、本装置の設定、ルート、log file、実行されたコマンド、などが含まれます。 この機能を使うことにより個別に必要な情報を収集するのに比べてはるかに速く情報を収集することができます。 これは、システムの起きた問題を報告することに役立ちます。
Backup configuration file	現在、稼働している設定ファイルを保存します。 設定ファイルを保存することは、本装置に誤った設定を行ったときや複数の装置に標準の設定を行う場合などに装置ごとに手動で設定を行う必要がなく Web interface で設定することができます。
Restore configuration from file	保存されている設定ファイルをアップロードします。
Installer radio test mode	この機能は使用しないでください。電波法違反になる恐れがあります。

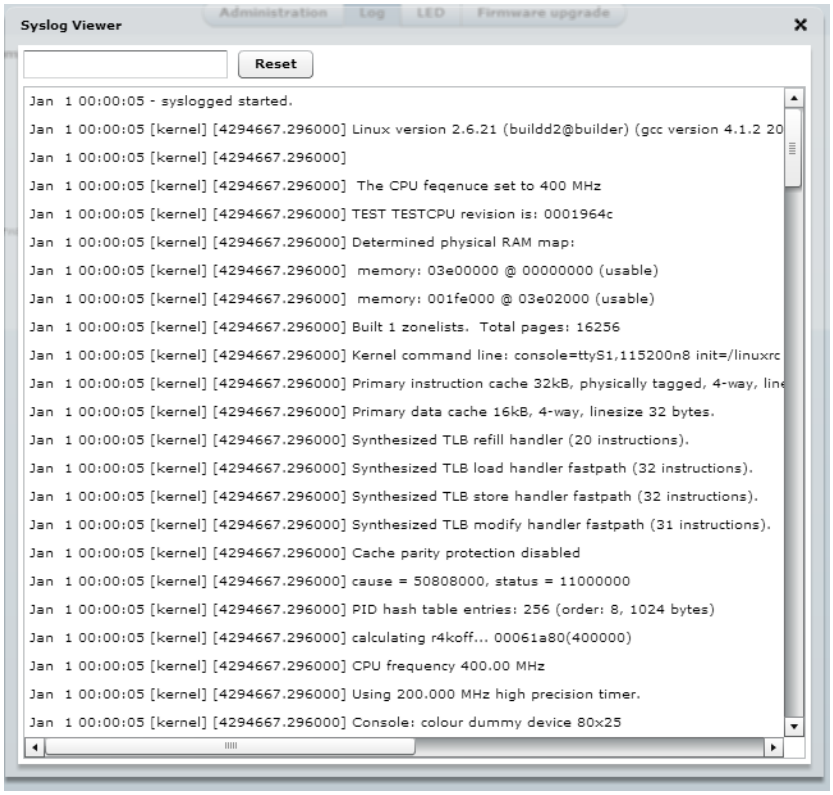
12.4.2. Log

Log tab でログメッセージの確認や保存する設定を行います。

ログメッセージは、標準の syslog 機能を利用してローカルあるいはリモートサーバに保存することができます。



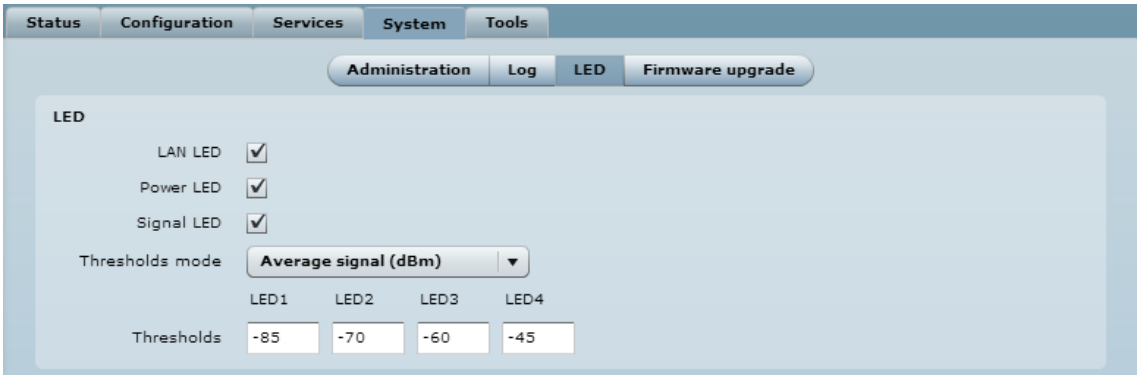
Syslog Viewer



項目	内容
View system log	View をクリックして現在のログデータを確認します。 System log viewer は、system service および protocol に ついてのデバッグ情報を提供します。 本装置に異常が発生したとき、保存された情報は設定の誤りやシステムエラーを特定することができます。
Message level	システムメッセージのトレースレベルを設定します。 このレベルは、本装置からのメッセージの重要性やメッセージのボリュームを決定します。 重要度が高くなるに従ってレベルが高くなります。 [emergency, alert, critical, error, warning, notice, information, debug] 初期値は、information です。
Syslog forward	system log 情報のリモートサーバへ転送機能を有効にします。
Forward server address	system log 情報を保存するサーバのホスト名あるいは IP アドレスを設定します。
Forward port	system log 情報を保存するサーバのポート番号を設定します [0-65535] 初期値:514
Forward message level	リモートサーバに転送するメッセージレベルを設定します。 このレベルは、本装置からのメッセージの重要性やメッセージのボリュームを決定します。 重要度が高くなるに従ってレベルが高くなります。 [emergency, alert, critical, error, warning, notice, information, debug] 初期値は、information です。
Forward backup	リモートサーバのバックアップ機能を有効にします。
Back server	バックアップサーバの IP アドレスあるいはホスト名を設定します。
Backup port	バックアップサーバのポート番号を設定します[0-65535 初期値:514

12.4.3. LED

本装置には、6 つの LED があります。電源、LAN および 4 つの RSSI 用の LED で、RSSI 用の LED は、現在の信号の強さを示しています。

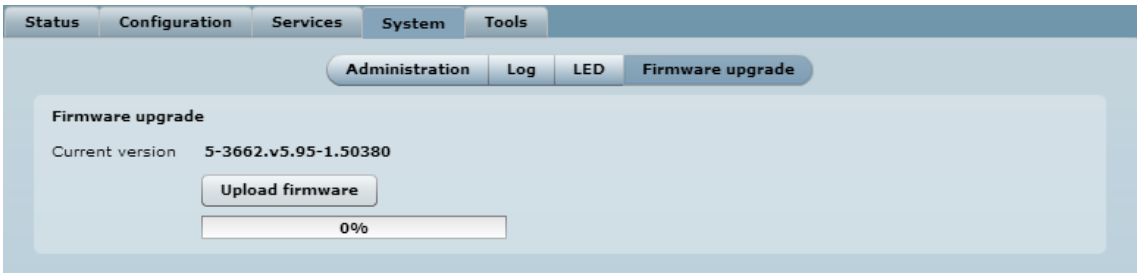


項目	内容
LAN LED	LAN LED 機能の有効/無効を選択します。 LED が緑色で点滅しているとき LAN 接続が確立しており、 LED が消灯しているときは LAN 接続が確立していません。
Power LED	Power LED 機能の有効/無効を選択します。 LED が緑色に点灯しているとき電源が on になっており、 LED が消灯しているとき電源は off になっています。
Signal LED	受信強度(RSSI)LED の有効/無効を選択します
Thresholds	Signal LED が点灯して切り替わる RSSI のしきい値を指定します。

12.4.4. Firmware upgrade

使用しているデバイスのファームウェアを更新する為に使用します。

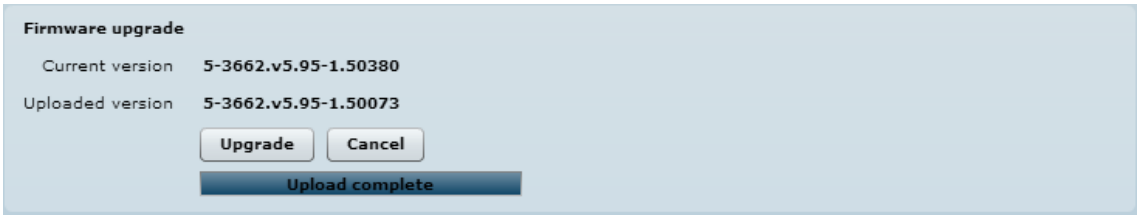
Update Firmware を押し、ファームウェアファイルを選択します。



項目	内容
Current version	現在のファームウェアバージョンが表示されます。
Upload firmware	このボタンをクリックし、アップロードするファームウェアイメージを選択します。

装置のファームウェアは、全ての設定に対して互換性があります。本装置を新しいバージョンまたは現在のバージョンでアップグレードしても全ての設定は影響を受けません。

新しいファームウェアイメージは、コントローラの一時メモリにアップロードされます。ファームウェアを固定メモリに保存する必要があります。



項目	内容
Upgrade	ファームウェアイメージをアップロードしシステムを再起動します。

本装置が故障する可能性がありますのでファームウェアのアップグレードの間に装置の電源を off にしないでください。

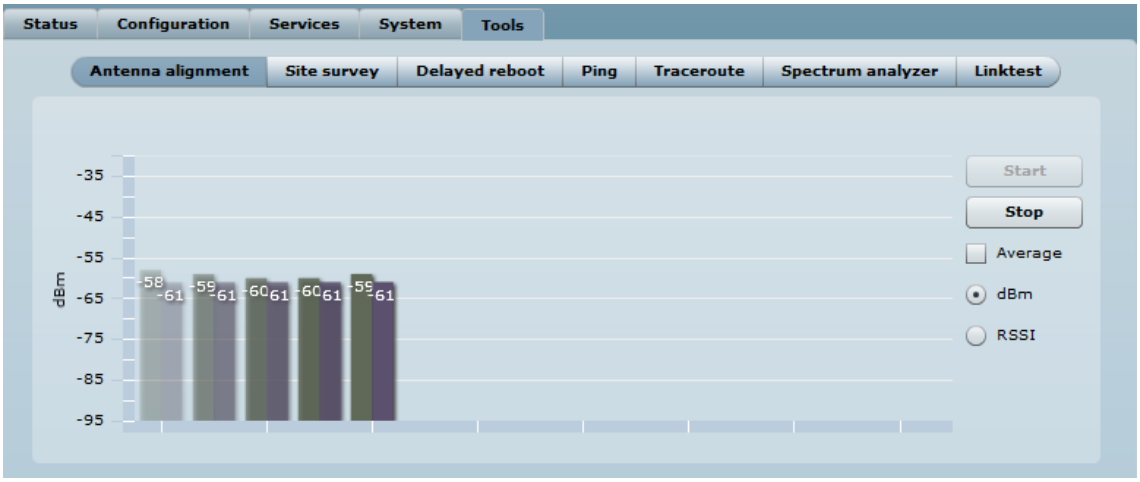
12.5. Tools

12.5.1. Antenna alignment

Antenna Alignment tool は、Station と AP 間のシグナル品質を測定します。

Antenna alignment test の良い結果が出るように他のワイヤレスネットワーク装置の Power を off にしてください。

アンテナを調整するとき antenna alignment test の結果を使用することができます。

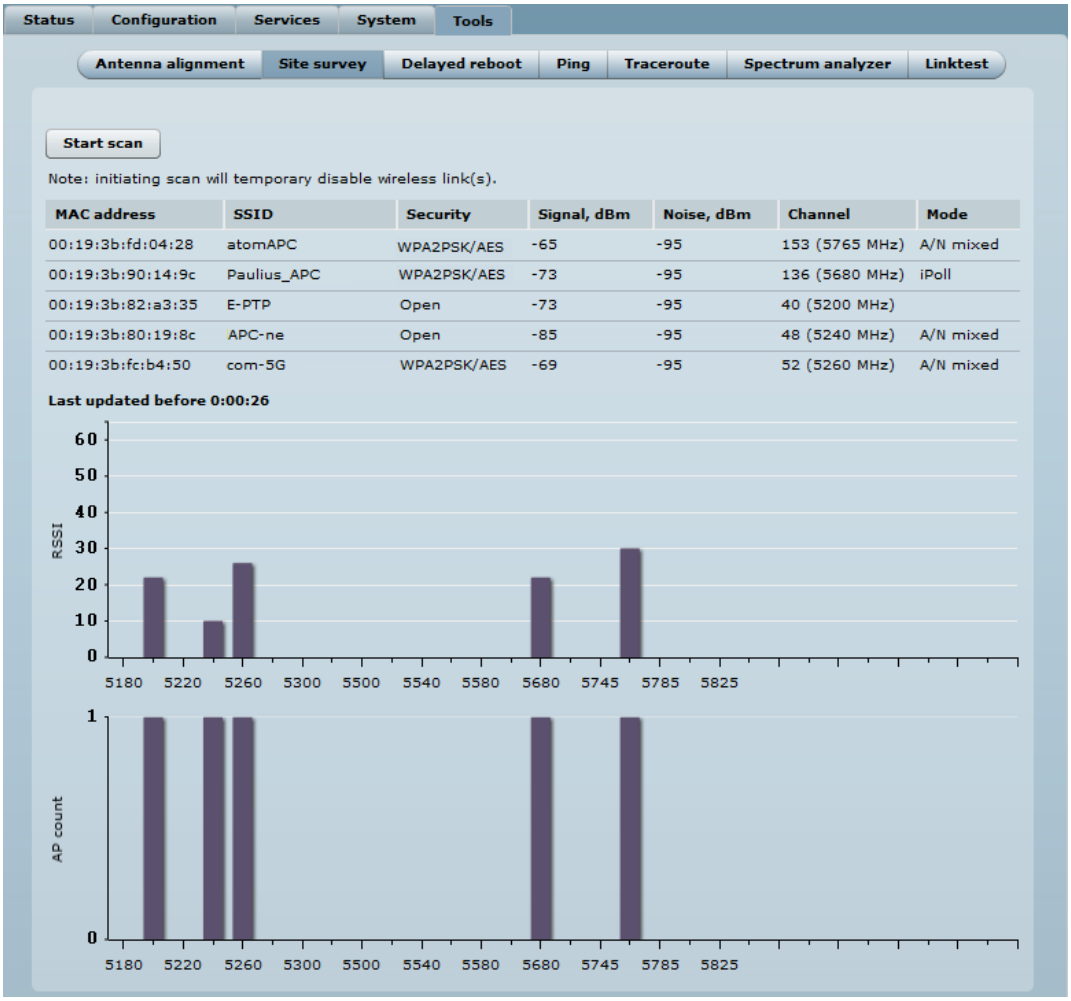


項目	内容
Start	このボタンをクリックして antenna alignment を開始します。
Stop	このボタンをクリックして antenna alignment を終了します。
Average	このボタンを有効にすると RSSI の平均値を表示します。

12.5.2. Site survey

Site Survey tool は、本装置を設置する周辺のワイヤレスネットワークに関する情報を表示します。このテストで稼働しているアクセスポイントを確認でき、そのアクセスポイントが利用しているチャネル、暗号化方式およびシグナルレベル/シグナルノイズレベルを確認することができます。

Start scan をクリックして Site Survey test を行います。



項目	内容
Last updated before	最後に scan したときの結果が表示されます。

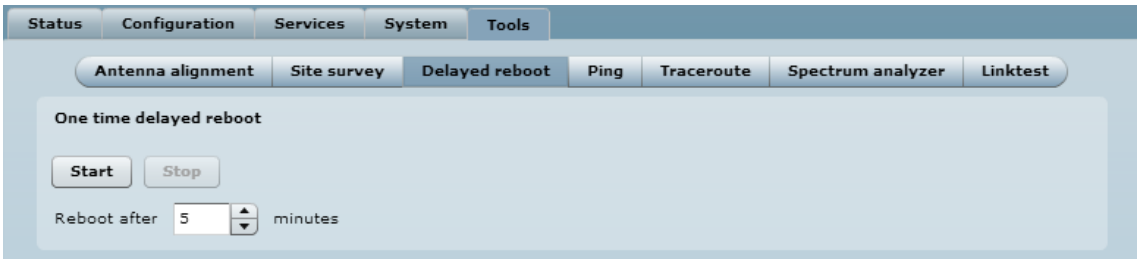
サイト調査試験の結果を便利な二つのグラフ(AP 数/RSSI)に変換されます。
管理者は、隣接する AP からの干渉を受けることはなく、デバイス動作のための最良のチャンネルを識別するために、これを使用します。

12.5.3. Delayed reboot

この機能は、特に radio 設定を調整する場合有効な機能です。

指定した時間でリブートを行います。この機能を使っている間は、設定を機器に保存できません。

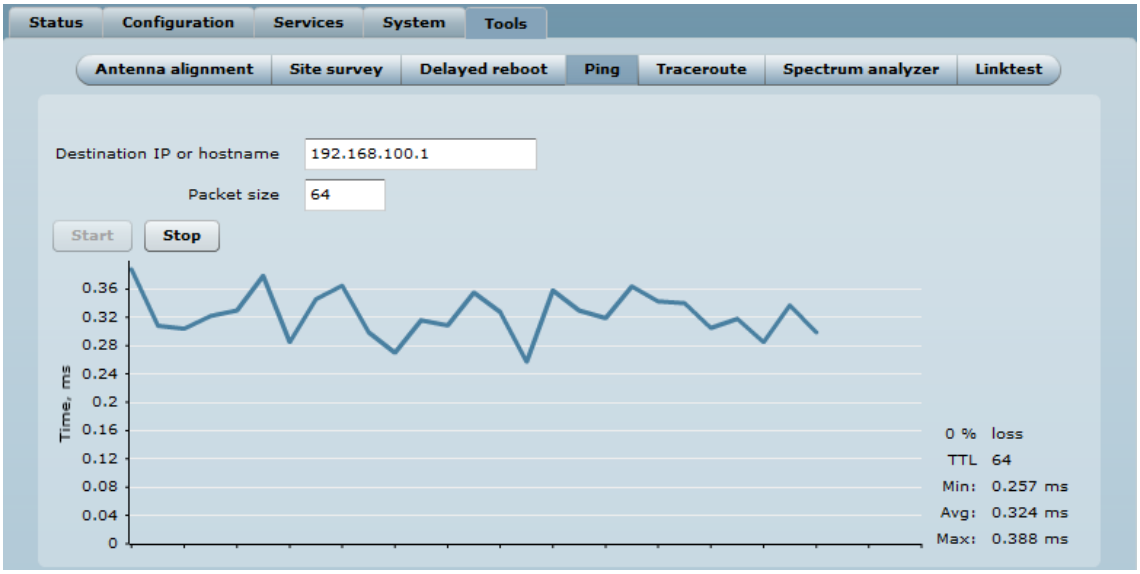
リブート後は、本機能を使う前の設定に戻ることになります。



項目	内容
Start/Stop	このボタンをクリックし遅延再起動の開始/停止を行います。
Reboot after	本装置が再起動するまでの時間を分単位で設定します。

12.5.4. Ping

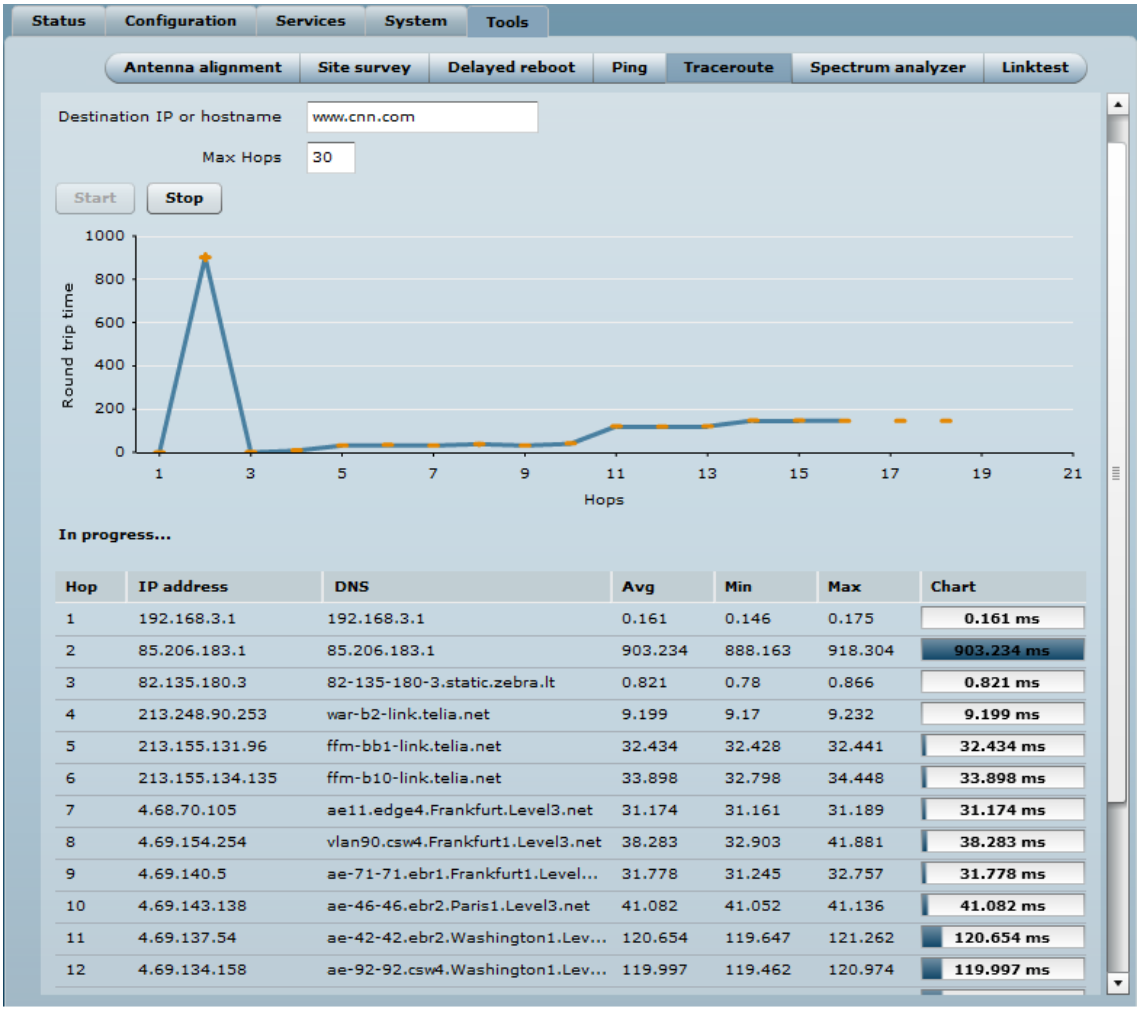
Ping コマンドは、本装置から特定のホストへ IP ネットワークを通してアクセス可能かどうかを確認するコマンドです。Ping 結果は、図表で表示されます。



項目	内容
IP address or Host name	宛先の IP アドレスあるいはホスト名を入力します。
Packet size	送信するパケットサイズを入力します。

12.5.5. Trance route

この機能は、IP パケットの送り宛先までのルートを確認する機能です。この機能を利用して、宛先へアクセスできない場合、ネットワークの故障個所を探索することができます。

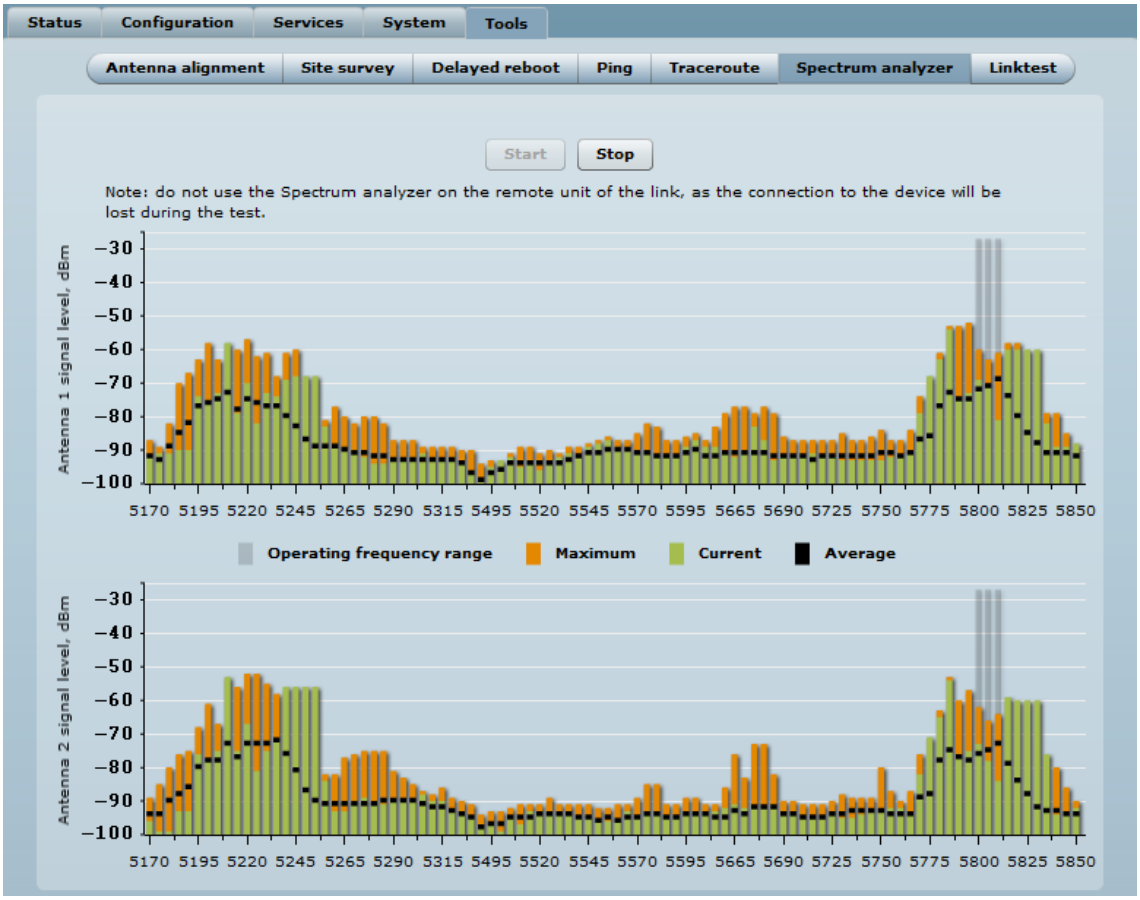


項目	内容
Destination	ターゲットホストのホスト名あるいは IP アドレスを入力します。
Max Hops	ターゲットホストへ到達するまでの最大ホップ数を入力します。
Start/Stop	このボタンをクリックし Trace route コマンドの Start/Stop を行います。

12.5.6. Spectrum analyzer

Spectrum analyzer test は、個々の AP の利用可能な周波数のシグナルレベルを表示します。
この情報により最適な周波数とチャネルを選択することができます。
周波数リストは、装置が運用される国およびチャネルの帯域により変わります。

Spectrum analyzer test をリモート装置を接続している link で行うとその接続がテストの間切れてしまいますので、この link に対してはテストを行はないでください。

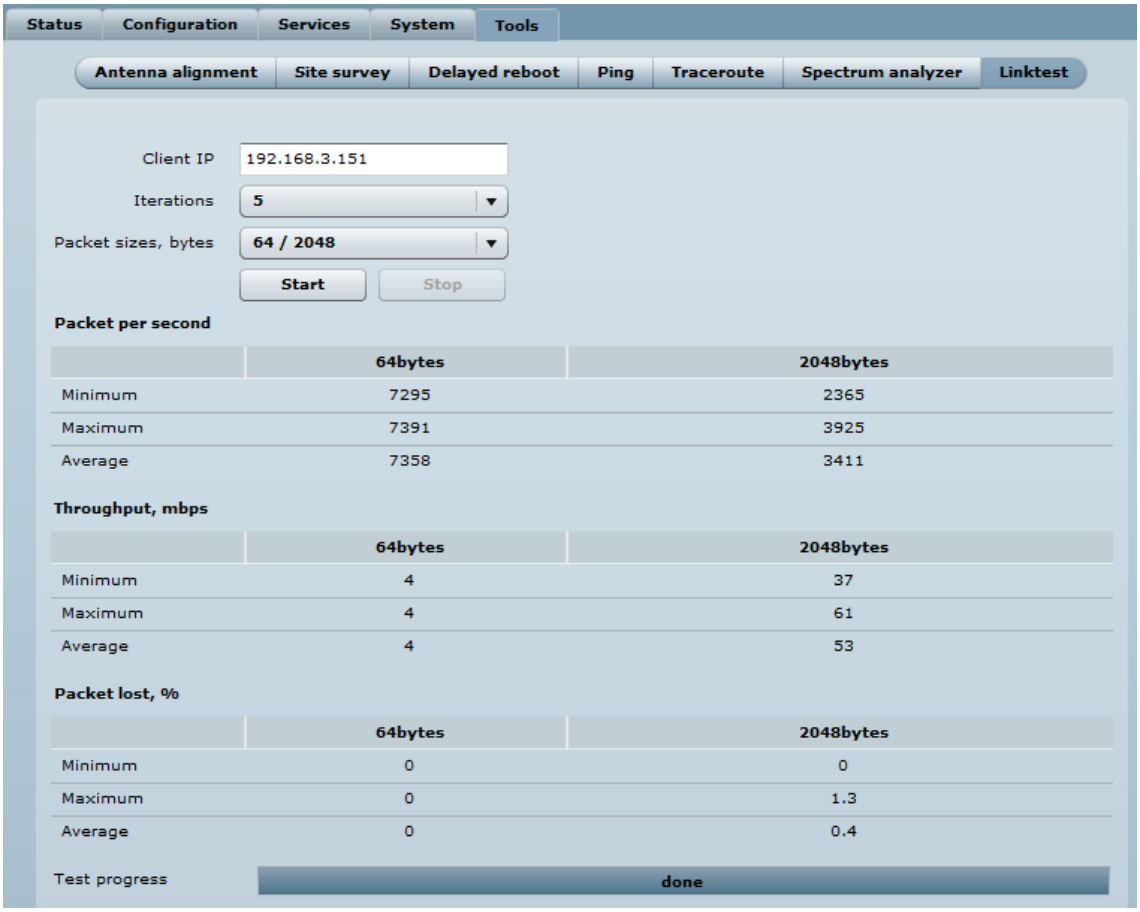


項目	内容
Operating frequency range	現在、AP が利用しているチャンネルの周波数の範囲を表示します。
Maximum	該当の周波数について最大シグナルレベルを表示します。
Current	該当の周波数について現在のシグナルレベルを表示します。
Average	該当の周波数について平均のシグナルレベルを表示します。

12.5.7. Link test

リンクテストを実行する前に結果が完全に正確ではない可能性があるので、
トラフィックがリンク上に存在しないことを保証することをお勧めします

確立されたリンクの品質をチェックするためにリンクテストツールを使用します。
このツールは、選択されたパケットサイズとの反復でのスループットをテストします。
結果は、実行されるテストの、最大値と最小値、平均値を表示します。



項目	内容
Client IP	接続されたクライアントの IP アドレスを指定します。
Iterations	テストの反復回数を指定します。
Packet sizes	テストが実行される時にバイト単位でのパケットサイズを指定します。
Start	スループットテストを開始するためにクリックします。
Stop	スループットテストを停止します。

13. ユニバーサルアクセス管理(UAM)

ユニバーサルアクセス管理(UAM)は、ウェブブラウザを用いたシンプルなユーザ認証方式です。最初にウェブサイトへ接続する時、クライアント側のブラウザはネットワークへログインするための認証ページへ移ります。ログインページは内部のウェブサーバもしくは外部のウェブアプリケーションサーバから提供されます。

13.1 UAM 概要

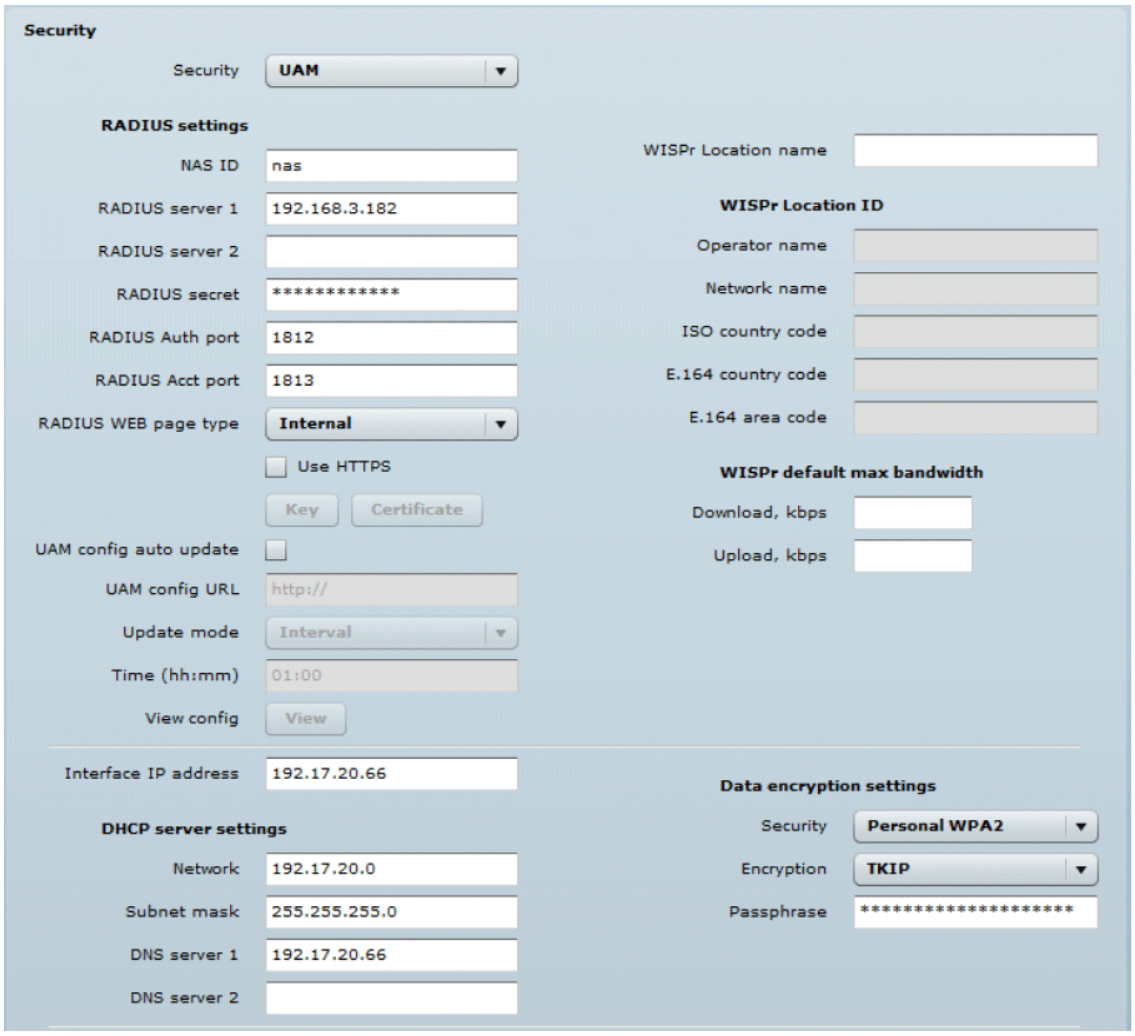
内部の UAM 機能を用いると、ユーザがウェブブラウザで URL 接続を行った際に、ログインページが最初のページとして表示されます。ネットワークへアクセスするためには、認証に必要なログインネームとパスワードを入力し、login ボタンをクリックする必要があります。

本製品は複数の無線インターネットサービスプロバイダ(WISP)とシェアすることが可能です。ログインの際に、ユーザネームに加え特定の WISP ドメインネームにより一意的にプロバイダが識別されます。本製品は、別の WISP ドメインに関連した AAA (Authentification, Authorization, Accounting)サーバに認証と承認とアカウンティングの情報の送信を設定することができます。

13.2UAM 設定

UAM 認証は本体が Access Point(auto WDS)モードでかつルータモードとして設定されている場合に限り無線インタフェース上(仮想 AP モードを含む)で用いることができます。

本製品は内部もしくは外部のウェブポータルを通してユーザ認証を行うことができます。この認証方式は UAM と呼ばれています。ユーザはログインの証明情報をウェブポータルへ提供し、ウェブポータル側は提供された情報を用いてクライアントの認証と承認を行います。クライアント側が認証要求を本製品へ直接送るのではなく、ウェブポータル側がこれを行うことになります。認証が成功すると、本製品はインターネットへの接続を承認し、失敗したときはウェブポータルが画面上にその旨を表示します。



Radius 設定

項目		内容
NAS ID		NAS ID を指定します。
RADIUS server 1		プライマリ RADIUS サーバの名前もしくは IP アドレスを指定します。
RADIUS server 2		セカンダリ RADIUS サーバの名前もしくは IP アドレスを指定します。
RADIUS secret		RADIUS 共有秘密キーを指定します。
RADIUS authentification port		RADIUS 認証要求で用いられる UDP ポート番号を指定します。デフォルト値は 1812 です。
RADIUS accounting port		RADIUS アカウント要求で用いられる UDP ポート番号を指定します。デフォルト値は 1813 です。
RADIUS WEB page type	認証ウェブポータルの種類を選択します。	
	Internal	内蔵の認証ウェブページを用います。ユーザが最初にインターネット接続を試みたときは、接続がブロックされ内蔵のログイン画面へ移ります。ログインデータは認証のため RADIUS サーバへ送られます。
	External	外部の認証用ウェブページの URL を指定します。ユーザが最初にインターネット接続を試みたときは、接続がブロックされ、設定された URL へ移ります。
	Custom internal	カスタマイズされた内部用ページをアップロードします。
Use HTTPS	接続と認証のための HTTPS プロトコルを用いるときはイネーブルにします。	
	Key	PEM 形式のプライベートキーファイルをアップロードします。
	Certificate	PEM 形式の証明ファイルをアップロードします。

WISPr の設定

項目	内容
WISPr location name	WISPr のロケーション名を指定します。
Operator name	オペレータ名を指定します。
Network name	ネットワーク名を指定します。
ISO country code	ISO 規格の国名コードを指定します。
E.164 country code	E.164 規格の国名コードを指定します。
E.164 area code	E.164 規格の地域コードを指定します。

WISPr default max bandwidth

クライアント側の帯域幅の制限値を指定します。外部の RADIUS サーバでトラフィック制限値が予め設定されている場合は、RADIUS がこの制限値を上書きすることに注意してください。

項目	内容
Download, kbps	ダウンロードの最大帯域幅を kbps 単位で指定します。
Upload, kbps	アップロードの最大帯域幅を kbps 単位で指定します。

UAM config auto update

UAM コンフィギュレーションの自動更新を選択します。イネーブルが選択された場合、本製品は決められた時間に決められた URL からコンフィギュレーションデータをダウンロードし適用します。

項目		内容
UAM config URL		UAM コンフィギュレーションデータのダウンロード元 URL を指定します。
Update mode	UAM コンフィギュレーションの自動更新モードを選択します。	
	Interval	決められた時間間隔で UAM コンフィギュレーションデータがダウンロードされ、本製品にセットされます。
	Time	毎日決められた時刻に UAM コンフィギュレーションデータがダウンロードされ、本製品にセットされます。
Time		時間もしくは時刻を hh:mm 形式で指定します。
Veiw coinfig		ダウンロードされたコンフィギュレーションファイルを見るときは、このボタンをクリックします。

Interface IP address

LAN インタフェースの IP アドレスを指定します。UAM がイネーブルになっているときは、Network メニューの LAN 設定は無効になっていることに注意してください。

DHCP 設定

接続したユーザ向けのダイナミック IP アドレス設定を指定します。

項目	内容
Network	IP アドレスが確保されているネットワークを指定します。
Subnet mask	DHCP 用のサブネットマスクを指定します。
DNS server	プライマリとセカンダリの DNS サーバを指定します。

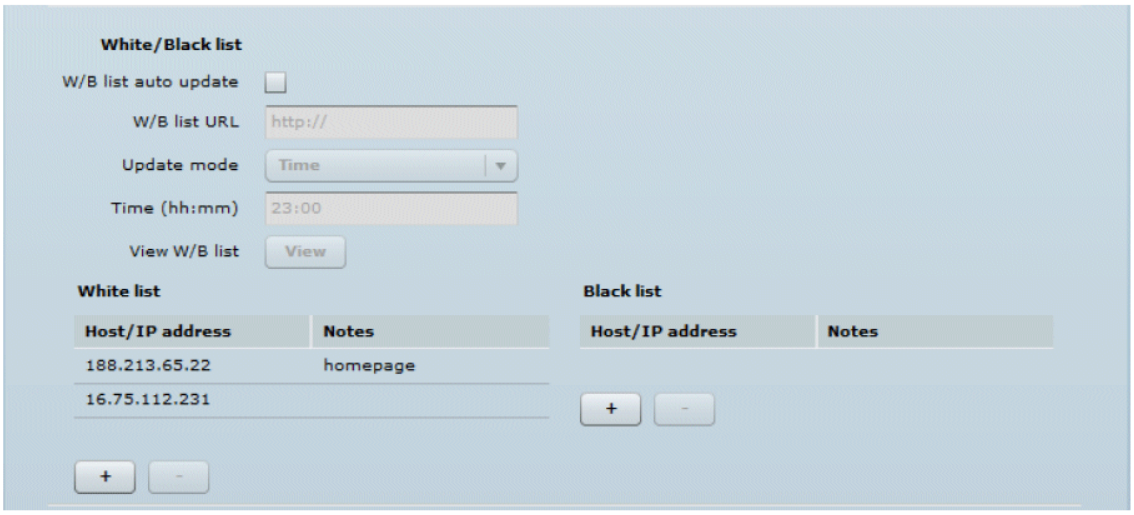
Data Encryption 設定

データ暗号化の方式を選択します。

項目	内容
Open	暗号化なし
Personal WPA	AES 方式を用いた WPA による事前共有キーで暗号化を行います。
Personal WPA 2	AES 方式を用いた WPA 2 による事前共有キーで暗号化を行います。

13.3ホワイト/ブラックリスト

ホワイト/ブラックアクセスリストでは、本製品を流れるウェブの内容に基づいてユーザのアクセスを制限します。ホワイトリストに載っているサイトへは、認証不要のユーザでもアクセスすることができます。一方、ブラックリストに載っているサイトへのアクセスは認証済みのユーザであっても拒否されます。



Web list auto update

ホワイト/ブラックリストの自動更新を選択します。イネーブルが選択された場合、本製品は決められた時間に決められた URL からホワイト/ブラックリストをダウンロードし適用します。

項目		内容
W/B list URL		ホワイト/ブラックリストのダウンロード元 URL を指定します。
Update mode	ホワイト/ブラックリストの自動更新モードを選択します。	
	Interval	決められた時間間隔でホワイト/ブラックリストがダウンロードされ、本製品にセットされます。
	Time	毎日決められた時刻にホワイト/ブラックリストがダウンロードされ、本製品にセットされます。
Time		時間もしくは時刻を hh:mm 形式で指定します。
Veiw coinfig		ダウンロードされたホワイト/ブラックリストを見るときは、このボタンをクリックします。

自動更新用ホワイト/ブラックリストの書式例

whitelist avp.innity.com,www.tm.com.my,m3.innity.net,pb2.ipass.com,

avn.innity.com,1.innity-.innity.net,tmpoint.tm.com.my,m4.innity.net

blacklist

ホワイト/ブラックリストの構築をマニュアルで行う場合は、新たにリストへ追加する場合は"+"の符号を使い、リストから削除する場合は"-"を使います。

White list

項目	内容
Host/IP address	認証要求をされないユーザでも自由にアクセスできる IP アドレスもしくはホスト名を指定します。
Notes	指定された IP アドレスもしくはホスト名に関する情報を記述します。

Black list

項目	内容
Host/IP address	認証を要求されたユーザでもアクセスできない IP アドレスもしくはホスト名を指定します。
Notes	指定された IP アドレスもしくはホスト名に関する情報を記述します。

AP Keep Alive Monitoring

AP キープアライブ機能により、指定されたリモート側サーバと接続が確保されているかをチェックすることができるようになります。

項目	内容
Enable monitoring	AP のキープアライブをモニタするときはイネーブルを選択します。
Monitor test URL	定期的にポーリングするリモート側装置の URL を指定します。
Interval	ポーリング間隔を hh:mm 形式で指定します。

14. 付録

14.1 工場出荷モードへの設定方法

本製品は、無線回線側が立ち上がるときに、適切なパケットサイズによる Ping を行うことで、工場出荷時の設定値へ戻せるようにする機能を持っています。本製品の立ち上げ時にイーサネットインタフェースのドライバがロードされるとDiscovery Daemon がスタートします。Daemon はスタートアップ処理を 3 秒間停止し、369 バイト長の ICMP ″echo request″パケットを待ちます。このパケットが受信されると Discovery は本製品をデフォルトの設定値にリセットします。

本製品をパソコンに接続するときはスイッチ経由で接続することをお勧めします。その際、パソコンの OS に基づいて、(リセットされる本製品が接続されている)有線系のリンクが変化している間に ARP テーブルをフラッシュしてください。

工場出荷モードへのリセット方法は次の通りです。

1. 本製品の電源をオフします。
2. 本製品の MAC アドレスを取得します。
3. 物理サブネットが本製品と同じであるパソコンを接続します。
4. IP アドレスを割り当てるため、本製品の MAC アドレスへ″arp -s″コマンドを送信してください。
   (IP アドレスはパソコンのサブネットと同じ範囲である必要があります。)
   arp -s <IP address to assign> <device MAC address>
   MAC アドレスの記述形式は OS によって異なることに注意してください。
   Linux OS: AA:BB:CC:DD:EE:FF
   Windows OS: AA-BB-CC-DD-EE-FF
5. 本製品へ Ping を送信します。
   Linux: ping <IP address> -s 369
   Windows: ping <IP address> -l 369 -t -w 200
6. 本製品の電源をオンし、30 秒以上(本製品のハードウェアによって異なります)待ちます。
7. Ping の送信を停止した後、通常の方法で本製品を立ち上げます。これにより、本製品は工場出荷モードで立ち上がります。

14.2 RADIUS 属性

本製品でサポートしている RADIUS 属性とメッセージは次の通りです。

一般属性

属性	内容
User-name (1)	ユーザがユーザネームをフルネームで入力します。
User-Password (2)	CHAP-Password と CHAP-CHallenge の代わりに UAM で使われます。
CHAP-Password (3)	UAM CHAP 認証用に使われます。
CHAP-Challenge (60)	UAM CHAP 認証用に使われます。
EAP-Message (79)	WPA 認証用に使われます。
NAS-IP-Address (4)	Chilli の IP アドレスです。(NAS IP または RADIUS listen のオプションにより設定されるか、もしくは"0.0.0.0"にセットされます。)
Service-Type (6)	通常の認証リクエスト用として Login(1)へセットします。設定管理メッセージ用 RADIUS サーバからの Access-Accept メッセージは Administrative-User へもセットする必要があります
Framed-IP-Address (8)	ユーザの IP アドレスです。Access-Accept で MAC 認証を行っているときに設定可能です。
Filter-ID (11)	スクリプトのよるフィルタ ID パスです。
Reply-Message (18)	拒絶した場合にその理由を示します。
State (24)	Access-Accept または Access-Challenge で Chilli へ送られます。続く Access-Request ではトランペアレントで使用されます。
Class (25)	Access-Accept から Accounting-Request まで Chilli によりトランスペアレントでコピーされます。
Session-Timeout (27)	セッションタイムアウト時間になるとログアウトします。(単位は秒です。)
Idle-Timeout (28)	アイドルタイムアウト時間になるとログアウトします。(単位は秒です。)
Called-Station-ID (30)	NAS MAC オプションまたは Chilli の MAC アドレスをセットします。
Calling-Station-ID (31)	クライアントの MAC アドレスです。
NAS-Identifier (32)	RADIUS NAS ID オプションがある場合にセットします。
Acct-Status-Type (40)	1=スタート, 2=ストップ, 3=仮のアップデート
Acct-Input-Octets (42)	クライアントから受信したオクテット数
Acct-Output-Octets (43)	クライアントへ送信したオクテット数

Acct-Session-ID (44)	Access-Request と Accounting-Request メッセージへリンクするための独自 ID です。
Acct-Session-Time (46)	秒単位によるセッション期間です。
Acct-Input-Packets (47)	クライアントから受信したパケット数です。
Acct-Output-Packets (48)	クライアントへ送信したパケット数です。
Acct-Terminate-Cause (49)	1=ユーザ要求、2=キャリア損失、4=アイドルタイムアウト、5=セッションタイムアウト、11=NAS 再起動
Acct-Input-Gigawords (52)	Acct-Input-Octets カウンタの回り込み回数です。
Acct-Output-Gigawords (53)	Acct-Output-Octets カウンタの回り込み回数です。
NAS-Port-Type (61)	19=Wireless-IEEE-802.11
Message-Authenticator (80)	常に Access-Request へ取り込まれます。 Access-Accept、Access-Challenge、Access-reject に存在する場合、 Chilli は Message-Authenticator が正常かどうかを検証します。
Acct-Interim-Interval (85)	Access-Accept に存在する場合、Chilli は指定された期間(秒単位)で仮のアカウンティングレコードを生成します。
MS-MPPE-Send-Key (311,16)	WPA で使用します。
MS-MPPE-Recv-Key (311,17)	WPA で使用します。

WISPr 属性

属性	内容
WISPr-Location-ID (14122, 1)	RADIUS ロケーション ID オプションが存在する場合、ローケーション ID をそこにセットします。書式は次のようにします。isocc=, cc≦E.164_Country_Code>, ac≦E.164_Area_Code>, network≦ssid/ZONE>
WISPr-Location-Name (14122, 2)	RADIUS ロケーション名のオプションが存在する場合、ローケーション名をそこにセットします。
WISPr-Logoff-URL (14122, 3)	Access-Request に組み込まれています。オペレータへログオフ URL を通知します。するために。デフォルト URL は次の通りです。" http://uamlisten:uamport/logoff".

WISPr-Redirection-URL (14122, 4)	この URL が存在する場合、クライアントは認証後にこの URL へ移ります。クライアントがログオフをできるようにするため、この URL には WISPr-Logoff-URL へのリンクが 含まれている必要があります。
WISPr-Bandwidth-Max-Up (14122, 7)	最大送信レート(単位は bps)です。接続時の帯域幅を制限します。
WISPr-Bandwidth-Max -Down (14122, 8)	最大受信レート(単位は bps)です。接続時の帯域幅を制限します。
WISPr-Session-Terminate -Time (14122, 9)	ユーザが接続を切断した時刻です。ISO 8601 の書式になります。(YYYY-MM-DDThh:mm:ssTZD) TZD が指定されていないときはローカル時間とみなされます。例えば、2001 年 12 月 18 日の午後 7 時 UTC に接続が切れた場合は、次のようになります。2001-12-18T19:00:00+00:00.

ChilliSpot 属性

属性	内容
ChilliSpot-Max-Input -Octets (14559, 1)	ユーザが送信できる最大オクテット数です。送信数がこの制限値に達するとユーザの接続は切断されます。
ChilliSpot-Max-Output -Octets (14559, 2)	ユーザが受信できる最大オクテット数です。受信数がこの制限値に達するとユーザの接続は切断されます。
ChilliSpot-Max-Total -Octets (14559, 3)	ユーザが送受信できる最大オクテット数です。送受信数がこの制限値に達するとユーザの接続は切断されます。
ChilliSpot-Bandwidth -Max-Up (14559, 4)	アップ側の最大帯域幅です。
ChilliSpot-Bandwidth -Max-Down (14559, 5)	ダウン側の最大帯域幅です。
ChilliSpot-Config (14559, 6)	ネームバリュー対として Chilli とバックエンド間でやりとりされた設定情報です。
ChilliSpot-Lang (14559, 7)	ユーザインタフェースで選択した言語です。
ChilliSpot-Version (14559, 8)	Access Request を送る Chilli のバージョンです。

15. 製品仕様

製品型番	APC 5M V3 4.9G/APC5M-12 V3 4.9G
無線 LAN インタフェース	IEEE802.11(a, j, n)
有線 LAN インタフェース	RJ-45(10/100BASE-TX) x1 ポート ・10/100BASE-TX Full/Half duplex の自動検出 ・オート MDI/MDI-X 機能
アンテナタイプ 利得 (APC 5M-12)	指向性パネルアンテナ 2T2R(MIMO) 4.9GHz 帯: 12 dBi
アンテナ部コネクタ 形状 (APC 5M)	N-Type メスコネクタ x2
セキュリティ	WEP、WPA/WPA2 Personal、WPA/WPA2 Enterprise、UAM
プロトコル	DHCP、SNMP、NTP、PPPoE、HTTP、HTTPS
変調技術	OFDM
変調方式	OFDM：16/64QAM、QPSK、BPSK
周波数帯	4.9- 5.0GHz
最大通信速度	802.11a(j)：54Mbps 802.11n(j)：300Mbps
チャンネル数	最大 10 チャンネル
SSID 登録数	8
無線動作モード	AP、Repeater、Station
最大送信出力	6dBm
受信感度	-95 ～ -75 dBm(変調方式による)
管理機能	HTTP/HTTPS、SNMP(read only) v1/v2c/v3
電源	AC 100～240V 50/60Hz（AC アダプタ） ※付属の専用 AC アダプタをご使用ください
最大消費電力	6.5W(最大)
動作温度	-40 ～ +65℃
動作湿度	0 ～ 90%（結露なきこと）
保存温度	-40 ～ +65℃
保存湿度	0 ～ 90%（結露なきこと）
寸法	(W)150mm x (D)115mm x (H)55mm(突起部含まず)
重量	400g(本体のみ)
取り付け方法	壁面マウント、支柱マウント
認定	TELEC(認定番号：208-150051) FCC、CE Marking、Safety、RoHS
製品保証期間	1 年間
付属品	挿入ブラケット、設置用ブラケット 結束バンド（10mm x 220mm） 壁設置用ねじ（M3.5 x 32）＆アンカー 専用 PoE アダプタ、AC 電源ケーブル

製品型番		APC 5M/APC 5M-12 専用 PoE アダプタ
有線 LAN インタフェース	24V PoE	RJ-45(10/100BASE-TX) x1 ポート
	LAN	RJ-45(10/100BASE-TX) x1 ポート
入力	定格入力電圧	AC100～240V 50/60Hz
出力	定格出力電圧	DC24V
	出力電圧範囲	DC24V±5%
保護機能		過電流保護、短絡保護
PoE 出力タイプ		Passive on 4,5(+) 7,8(−)ピン
動作温度		−10～+50℃
寸法		(W)85mm x (D)44mm x (H)30mm(突起部含まず)
重量		95g(本体のみ)
規格・認定		PSE、IEC320 C6
製品保証期間		1 年間

※本製品にはリピータ機能はありません。ネットワーク機器 − APC 5M 間の LAN ケーブル長の合計は 100m までとなります。

16. 製品保証

◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
2) 本製品の保証期間内の自然故障につきましては無償修理させて頂きます。
3) 故障の内容により、修理ではなく同等品との交換にさせて頂く事があります。
4) 弊社への送料はお客様の負担とさせて頂きますのでご了承ください。

初期不良保証期間:

ご購入日より **3ヶ月間**（弊社での状態確認作業後、交換機器発送による対応）

製品保証期間:

ご購入日より **1年間**（お預かりによる修理、または交換対応）

◆ 保証期間内であっても、以下の場合は有償修理とさせて頂きます。
（修理できない場合もあります）

1) 使用上の誤り、お客様による修理や改造による故障、損傷
2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
3) 本製品に水漏れ・結露などによる腐食が発見された場合

◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。

◆ 本製品に起因する損害や機会の損失については補償致しません。

◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。

◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社
カスタマサポート
TEL 0570-060030
MAIL support@hytec.co.jp
受付時間 平日 9:00～17:00

Copyright © 2015
HYTEC INTER Co., Ltd.